ELABORACIÓN DE GUÍAS DE LABORATORIO SOBRE IPV6 BASADOS EN UN SOFTWARE DE SIMULACIÓN

DIRECTOR DEL PROYECTO:

PH.D JHON JAIRO PADILLA AGUILAR

INVESTIGADORES:

Soranyeli Mancera Meza

Jenny Marcela Ardila Cruz

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE INGENIERÍAS Y ADMINISTRACIÓN

BUCARAMANGA

2010

ELABORACIÓN DE GUÍAS DE LABORATORIO SOBRE IPV6 BASADOS EN UN SOFTWARE DE SIMULACIÓN

SORANYELI MANCERA MEZA
JENNY MARCELA ARDILA CRUZ
Estudiantes de Ingeniería Electrónica

Trabajo de grado presentada como requisito para optar el título de Ingeniero Electrónico

DIRECTOR DEL PROYECTO:
JHON JAIRO PADILLA AGUILAR, PhD.

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍAS Y ADMINISTRACIÓN
FACULTAD DE INGENIERÍA ELECTRÓNICA
2010

Nota de aceptación

_____
_____
_____
_____

_____

Firma del Jurado

_____

Firma del Jurado

Bucaramanga, Julio del 2010

DEDICATORIA

Dedico este trabajo a Dios que me iluminó constantemente, mostrándome el camino y rumbo de mi vida.

A mis padres Oswaldo Mancera y Rocio Meza, que me han apoyado en momentos difíciles y que han sonreído conmigo en los felices y por contar con su amor incondicional.

A mi Hermana Larisa Mancera, a mi tía Luz Estela Meza y a mi Nona Hilma Pinzón, por cada consejo y confianza que han depositado en mí, brindándome las fuerzas suficientes para seguir en la lucha de mis ideales**.**

DEDICATORIA

A Dios por iluminarme el camino a seguir.

A mi mamá y mi papá por el apoyo incondicional en cada etapa de mi vida.

A mi ahijada por regalarme su sonrisa y mirada inocente.

Jenny Marcela Ardila Cruz

AGRADECIMIENTOS

A nuestro director Jhon Jairo Padilla Aguilar por su apoyo incondicionalidad para con nosotras.

A la universidad por brindarnos todo aquel conocimiento para nuestra vidas en un futuro y por la formación integral.

A todos aquellos que de una u otra forma nos colaboraron en la realización del proyecto de grado.

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

IP: (Internet Protocol) Este protocolo permite la comunicación entre equipos que estén conectados por la misma red, pues es el encargado de transportar paquetes desde el origen al destino. En el caso de Internet se pueden conectar muchos usuarios y poder cambiar información entre ellos.

IPv4: Es la versión 4 del Protocolo IP, que tiene como característica direcciones de 32 bits, son 4.294.967.296 direcciones disponibles.

IPv6: Es una nueva versión del protocolo IP, diseñada para reemplazar a IPv4 cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso provee direcciones de 128 bits disponibles.

Enrutamiento: El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino.

Protocolo de enrutamiento: Un protocolo de enrutamiento es el que define el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento.

Protocolo enrutado: Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un host a otro, basado en el esquema de direcciones.

QoS: A la capacidad de una red para asegurar una cantidad de recursos y diferenciar servicios se le conoce como *Calidad de Servicio* (*QoS, Quality of Service*).

DiffServ: Servicios Diferenciales, fue desarrollada en respuesta a la necesidad de métodos toscos pero simples de proveer diferentes niveles de servicio para el tráfico de *Internet* y para soportar diferentes tipos de aplicaciones y negocios específicos.

Best effort: Es un servicio que se basa en la entrega de paquetes mediante la técnica considerada como de mejor esfuerzo.

Latencia: Tiempo de retardo en la transmisión y propagación de paquetes de datos en una red.

WFQ (Weighted Fair Queuing): Planificador con prioridades.

Mobile Node (MN): Nodo que puede cambiar su punto de acceso entre los diferentes puntos de acceso de diferentes redes, mientras permanece localizado con su home address.

Home address: Dirección asignada a un MN, usada para comunicarse con el MN aunque éste no se encuentre en su red de origen.

Correspondent Node (CN): Nodo con el que se está comunicando el MN, éste puede ser móvil o no.

Care-of-Address (CoA): Dirección asociada a un MN mientras está visitando una red que no es la de origen.

Home Agent (HA): Router de la red de origen del MN en la que está registrada la dirección actual de CoA.

Binding: Asociación de una dirección dada por la red de origen del MN y la [illegible], que permanece durante el tiempo de vida de la asociación.

Registration: El proceso durante el que el MN envía un Binding Update a su HA o CN, para que se realice el binding y así se registre el nodo.

RESUMEN GENERAL DE TRABAJO DE GRADO

TITULO: ELABORACIÓN DE GUÍAS DE LABORATORIO SOBRE IPV6 BASADOS EN UN SOFTWARE DE SIMULACIÓN

AUTORES: SORANYELI MANCERA MEZA
JENNY MARCELA ARDILA CRUZ

FACULTAD: INGENIERIA ELECTRÓNICA

DIRECTOR: PH.D JHON JAIRO PADILLA AGUILAR

RESUMEN

En este trabajo de grado se realizaron guías de laboratorio para estudiar el nuevo protocolo de Internet IPv6. Para esto se llevó a cabo el estudio de los contenidos correspondientes y aplicaciones que este encierra.

Las guías se hicieron con el fin de orientar a los estudiantes en el estudio de nuevos mecanismos de transición y los diferentes temas como calidad de servicio, seguridad y movilidad. En el desarrollo de las prácticas se explica paso a paso la configuración de los diferentes dispositivos.

Se eligió OPNET MODELER como simulador, ya que encierra ampliamente la temática de IPv6. Además, tiene herramientas claves para la realización de los laboratorios y el análisis completo de aspectos como: tráfico de la red, ancho de banda y parámetros que miden de una u otra forma el funcionamiento de la red.

PALABRAS CLAVES: simulación, redes de nueva generación, internet, OPNET MODELER, IPV6

GENERAL SUMMARY OF WORK OF DEGREE

TITLE: DEVELOPMENT OF IPV6 LAB MANUAL BASED ON A SIMULATION SOFTWARE

AUTHORS: SORANYELI MANCERA MEZA
JENNY MARCELA ARDILA CRUZ

FACULTY: ELECTRÓNIC ENGINEERING

DIRECTOR: PH.D JHON JAIRO PADILLA AGUILAR

ABSTRACT

This undergraduate project performace a laboratory manual to study the new IPv6 Internet protocol. Here, the study of the several was done focused in the designated applications that IPv6 enclose it.

The lab practices were developed to guide the students to implement the new IPv6/IPv4 transition mechanisms and other topics including quality of service, security and mobility. The body of the practices explains step by step the configuration of the different devices.

The OPNET MODELER simulator was choose because it widely involves the IPv6 protocol and it has the necessary key tools to conduct the lab practices with full analysis of several topics like: network traffic, bandwidth and other userful measuring parameters required to control the operation of an IPv6 network.

KEY WORDS: IPV6, OPNET MODELER, simulation, next generation, networks, internet

1. INTRODUCCIÓN

En la actualidad se maneja un Internet de protocolo versión 4 (IPv4) que proporciona un servicio no muy eficiente, ya que con el pasar del tiempo se ha incrementado el número de habitantes y por ende el número de usuarios que utilizan el servicio de internet. El uso de la tecnología como redes inalámbricas, redes domésticas, sistemas de seguridad, de control, de televisión y radio basado en IP y las innumerables aplicaciones que necesitan direcciones IP han tenido una revolución muy importante; esto ha requerido que se implemente una nueva versión, conocida como el protocolo versión 6 (IPv6) para lograr obtener varios servicios con una alta eficiencia, con mejores rutas para enviar los paquetes de forma rápida, con alta calidad de forma segura y sobre todo con un mayor número de direcciones, que permitirán realizar mejores aplicaciones y estar en auge con el crecimiento tecnológico.

Este es el inicio de una investigación amplia acerca de este nuevo protocolo cuya utilización es inminente. IPv6 proporciona ventajas y beneficios que mejoran algunos problemas que tiene su antecesor IPv4, y ayuda a los usuarios de las comunicaciones a evolucionar de una manera rápida. Pero para llegar a esto se debe trabajar e implementar formas de familiarización y migración hacia este nuevo protocolo de comunicaciones.

La idea principal es lograr utilizar las características y la flexibilidad que ofrece IPv6 para realizar un manejo adecuado y lograr acercar al estudiante a esta tecnología.

1.1. OBJETIVOS GENERALES

- Diseñar y realizar prácticas de laboratorio sobre IPv6 y los diferentes temas que son de utilidad en este campo, utilizando un simulador de redes.
- Desarrollar prácticas de simulación que permitan estudiar los temas mencionados en los objetivos.

1.2. OBJETIVOS ESPECÌFICOS

- Analizar la teoría básica acerca de IPv6 y los diferentes temas que esta encierra; (Calidad de Servicio, Seguridad, Movilidad, etc).
- Estudiar los mecanismos de transición de IPv4 a IPv6.

2. PROTOCOLO DE INTERNET VERSIÒN 4

2.1. GENERALIDADES

IP es el mecanismo de transmisión utilizado por los protocolos *TCP/IP.* Es un protocolo basado en datagramas sin conexión y no fiable, ofrece un servicio de mejor entrega posible *(Best Effort)*. Por mejor entrega posible, se quiere indicar que *IP* no ofrece comprobaciones ni seguimientos. *IP* asume que los niveles subyacentes no son fiables e intenta que la transmisión llegue a su destino. Las transmisiones a través de redes físicas pueden ser destruidas por varios motivos. El ruido puede causar errores en los *bits* durante la transmisión por el medio, un encaminador congestionado puede descartar un datagrama si es incapaz de retransmitirlo antes que se supere un límite de tiempo; el encaminamiento puede hacer que los datagramas entren a un bucle y sean destruidos finalmente, y los enlaces desactivados pueden hacer que no haya camino para alcanzar al destino.

IP transporta los datos en paquetes denominados datagramas, cada uno de los cuales es transportado de forma independiente. Los datagramas pueden viajar a través de encaminadores diferentes y llegar fuera de secuencia o duplicados. *IP* no se encarga de realizar un seguimiento de los encaminadores ni ofrece facilidades para reordenar los datagramas una vez recibidos. Debido a que es un servicio sin conexión, *IP* no crea circuitos virtuales para la entrega.[1] No hay un establecimiento de llamada que indique al receptor la llegada de una transmisión.
La funcionalidad limitada de *IP* no debería ser considerada como una debilidad, sin embargo, *IP* ofrece funciones de transmisión básicas y deja la libertad al usuario para añadir sólo aquellas facilidades necesarias para una aplicación concreta, permitiendo por tanto una máxima eficiencia y flexibilidad.

[1] BEHROUZ A FOROUZAN. *Transmisión de Datos y Redes de Comunicaciones.* 2da edición. 2002. *Mc Graw Hill*.

2.1.1 Partes del Datagrama *IPv4*

Los paquetes en el nivel *IP* se denominan datagramas. La figura 1 (datagrama *IPv4*), muestra el formato de un datagrama *IP*. Un datagrama es un paquete de longitud variable (hasta 65.536 *bytes*), que consta de dos partes: una cabecera y datos. La cabecera puede incluir de 20 a 60 *bytes* y contiene información esencial para el encaminamiento y la entrega. Es habitual en *TCP/IP* mostrar la cabecera en secciones de cuatro *bytes*. A continuación se realiza una breve descripción de cada campo:

- **Versión**: El primer campo define el número de versión de *IP.* La versión actual es la 4 (*IPv4*), con u valor binario de 0100.

- **Longitud de la cabecera**: Este campo define la longitud de la cabecera en múltiplos de cuatro *bytes*. Cuatro *bits* pueden representar un número entre 0 y 15, que cuando se multiplica por 4 da un máximo de 60 *bytes.*

- **Tipo de servicio**: Este campo define la forma en la que se debería manejar el datagrama. Incluye *bits* que definen la prioridad del datagrama. También contiene *bits* que especifican el tipo de servicio que el emisor desea como el nivel de prestaciones, fiabilidad y retardo.

- **Longitud total**: El campo con la longitud total define la longitud total del datagrama *IP*. Es un campo de dos *bytes* (16 *bits*), que puede definir hasta 65.536 *bytes.*

- **Identificación**: Este campo se utiliza en la fragmentación. Un datagrama, cuando pasa a través de redes diferentes, puede dividirse en fragmentos

que coincidan con el tamaño de una trama de red. Cuando esto ocurre, cada fragmento es identificado con un número de secuencia en este campo.

- **Indicadores**: Los *bits* de este campo están relacionados con la fragmentación (el datagrama puede estar o no fragmentado; puede ser el primero, el último fragmento, etc.).

- **Desplazamiento del fragmento**: El desplazamiento del fragmento es un puntero que muestra el desplazamiento de los datos en el datagrama original (si se fragmenta).

- **Tiempo de vida**: El campo de vida define el número de saltos que un datagrama puede dar antes de que sea descartado. La estación origen, cuando crea el datagrama, fija este campo a un valor de 1. Si el valor se hace 0 antes que el datagrama haya alcanzado el destino final, se descarta el datagrama. Esto evita que un datagrama vuelva o viaje de forma indefinida entre caminadores.

- **Protocolo**: Este campo define el protocolo de nivel superior que se encuentra encapsulado en el datagrama (*TCP, UDP, ICMP,* etc.).

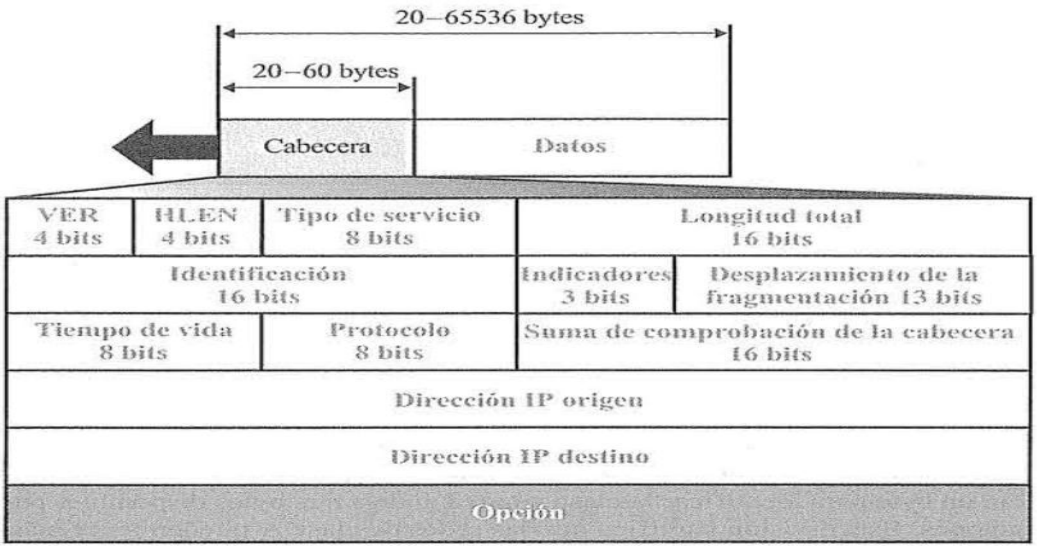
- **Suma de comprobación de la cabecera**: Este campo de 16 *bits* se utiliza para comprobar la integridad de la cabecera, no del resto del paquete.

- **Dirección origen:** El campo con la dirección origen es una dirección de internet de 4 *bytes* (32 *bits*). Identifica el origen del datagrama.

- **Dirección destino:** Este campo es una dirección de internet de 4 *bytes* (32 *bits*). Identifica el destino del datagrama.

- **Opción:** El campo de opciones ofrece más funcionalidad al datagrama *IP*. Puede transportar datos que controlan el encaminamiento, la temporización, la gestión y el alineamiento. [2]

Figura 1. Datagrama IPv4



FUENTE: [1]

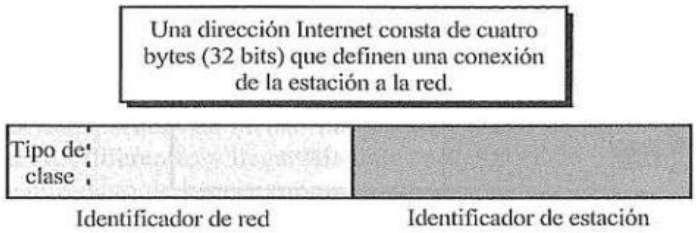
2.1.2 Direccionamiento

Además de la dirección física (contenida en la interfaz de red) que identifica el dispositivo individual, Internet requiere una convención en el direccionamiento: una dirección que identifique la conexión de una estación a la red.

Cada dirección de red, consta de cuatro *bytes* (32 *bits*), que definen tres campos: la clase, el identificador de la red y el identificador de la estación. Estas partes son de longitud variable dependiendo de las clases de direcciones. [3]

[2] BEHROUZ A FOROUZAN. *Transmisión de Datos y Redes de Comunicaciones.* 2da edición. 2002. *Mc Graw Hill*.

Figura 2. Dirección Internet



Fuente: [1]

[3] BEHROUZ A FOROUZAN. *Transmisión de Datos y Redes de Comunicaciones.* 2da edición. 2002. *Mc Graw Hill*.

3. PROTOCOLO DE INTERNET VERSIÒN 6

3.1 GENERALIDADES

A principios de la década de 1990, el IETF (internet engineering task forcé) abordo el proyecto de desarrollar un sucesor para el protocolo IPv4. El principal motivo del esfuerzo fue el hecho de que el espacio de direcciones IP de 32 bits estaba comenzando a agotarse, al añadir a marchas forzadas redes y nodos IP (para cada uno de los cuales se precisaba de una única). Para responder a esta necesidad de un gran espacio de direcciones IP, se desarrollò un nuevo protocolo IP: IPv6. Los diseñadores de IPv6 aprovecharon también esta oportunidad para retocar y aumentar ciertos detalles de IPv4, basándose en la experiencia acumulada con la operación de IPv4.

Cuál sería el momento en que el espacio de direcciones de IPv4 estaría completo (y por tanto no se podían enlazar nuevas redes de Internet) fue un tema de considerable debate. Basándose en las tendencias de asignación de direcciones de la época, las estimaciones de los dos líderes del grupo de trabajo de IETF Address lifetime Expectations (esperanza de vida de direcciones) concluyeron respectivamente que las direcciones se agotarían en 2008 y 2018. En 1996, el registro Americano para números de Internet (ARIN; American Registry for internet number) informó que ya se habían asignado todas las direcciones IPv4 de clase A, el 62% de las clases B, y el 37% de las direcciones de la clase C. Aunque estas estimaciones y números sugirieron que aun quedaban una cantidad de tiempo considerable para agotar el espacio de direcciones IPv4, quedó claro que se precisaría mucho tiempo para desplegar una nueva tecnología en tamaña escala, por lo que se abordó la iniciativa "IP de la próxima generación" (IPng; Next generation IP), el resultado de la iniciativa fue la especificación de la versión 6 de IP (IPv6). [2]

3.1.1 Partes del Datagrama IPv6

- *Capacidad de direccionamiento extendida.* IPv6 incrementa el tamaño de las direcciones IP de 32 a 128 bits. Esto asegura que el mundo no agotara las direcciones IP. Ahora, cada grano de arena del planeta es IP-direccionable. Además de las direcciones de unidifusión hacia un punto (unicast) y el multidifusión (multicast), IPv6 ha introducido un nuevo tipo de direcciones, denominados direcciones anycast (difusión hacia algún enlace), que permiten dirigir un datagrama a una dirección, (Esta característica se utilizara, por ejemplo, para enviar un mensaje HTTP GET al más próximo de un grupo de servidores en espejo (mirror) que contuvieron cierto documento).

- *Cabecera de 40-bytes estilizada*. Como se verá a continuación, se han eliminado o convertido en opcionales ciertos campos de IPv4. La cabecera resultante, de longitud fija de 40 bits, permite un procesamiento más rápido de datagrama IP. Un nuevo esquema de codificación de opciones permite un procesamiento de las opciones flexible.

- *Etiquetado de flujo y prioridad.* IPv6 tiene una definición un tanto elusiva de flujo la RFC 1752 Y 2460 sostiene que esto permite “etiquetar los paquetes pertenecientes a ciertos flujos para los cuales el emisor espera un tratamiento especial, como una calidad de servicio mejorada o un servicio de tiempo real”. Por ejemplo, la transmisión de sonido y video seria tratada mejor como un flujo. Sin embargo, ciertas aplicaciones más tradicionales, como la transferencia de archivos el correo electrónico, no tendrían por qué tratarse como flujo. Es posible que el tráfico transmitido por un usuario de alta prioridad, (por ejemplo, alguien que pagara por un mejor servicio para su tráfico) pudiera ser tratado también como un flujo. Prevén la necesidad

eventual de diferenciar entre los flujos, incluso aunque el significado exacto de tal característica no haya sido determinado aún. La cabecera de IPv6 también tiene campos de case de trafico de 8 bits. Este campo, como el campo de TOS de IPv4, puede usarse para priorizar los datagramas de ciertas aplicaciones (por ejemplo los paquetes ICMP) sobre los datagramas de otras aplicaciones (por ejemplo la red de noticias).[2]

En IPv6 se definieron los siguientes campos:

- **Versión:** Este campo de 4 bits identifica el número de versión de IP. No es sorprendente que en IPv6 este campo lleve un valor de 6.

- **Clase de tráfico**: Como ya se discutió, este campo de 20 bits se emplea para identificar un flujo de datagramas.

- **Longitud de datos:** Este valor de 16 bits se trata como un entero sin signo que plasma el número de bytes del datagrama IPv6 que acompañan a los 40 bytes de cabecera, de longitud fija.

- **Siguiente cabecera:** Identifica el protocolo hacia el que se dirigen los contenidos (campo de datos) de este datagrama (por ejemplo, hacia TCP o UDP). Este campo emplea los mismos valores que en el campo de protocolo de la cabecera IPv4.

- **Limite de Saltos:** El contenido de este campo se decrementó en uno cada vez que el datagrama es encaminado por un router. Si el contador de límite de saltos llega a cero, se desecha el datagrama.

- **Direcciones Fuente y destino:** Los diversos formatos de direcciones de IPv6 de 128 bits de longitud se describen en RFC 2373.

- **Datos:** Esta es la zona de carga (payload) del datagrama IPv6. Cuando el datagrama llega a su destino, se extrae la carga del datagrama IP y se pasa al protocolo especificado en el campo de siguiente cabecera.

Las definiciones anteriores señalaban el contenido de los campos que están incluidos en el datagrama IPv6. Al comparar el formato de datagrama de IPv6 con el formato de IPv4, se observa que ciertos campos que figuraban en el datagrama IPv4 ya no aparecen en el datagrama IPv6.[2]

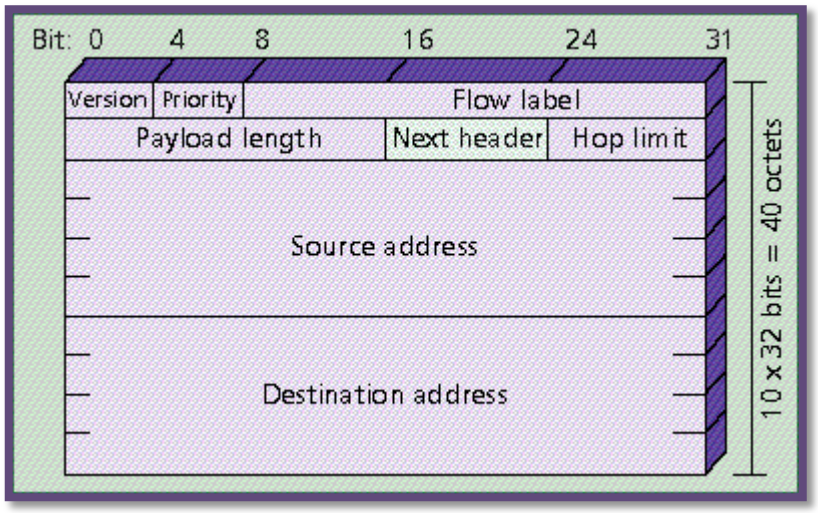
- *Fragmentación/reensamblado.* IPv6 no permite la fragmentación y el reesamblado en routers intermedios. Estas operaciones solo podrán hacerse en la fuente y el destino. Si el datagrama IPv6 recibido en un router resulta demasiado grande para ser encaminado por cierto enlace de salida, el router simplemente desecha el datagrama y envía de vuelta al emisor el mensaje ICMP de error “Paquete demasiado grande” (packet too big). El emisor podrá después enviar datos, usando un menor tamaño de datagrama IP. La fragmentación y el reemblado son operaciones onerosas. Al eliminar de los routers esta funcionalidad y ubicarla directamente en los sistemas finales, se acelera el encaminamiento IP en la red.

- *Suma de comprobación de la cabecera.* Puesto que los protocolos de la capa de transporte (por ejemplo TCP y UDP) y de la de enlace de datos (por ejemple Ethernet) de Internet realizan funciones de suma de comprobación, los diseñadores de IP pensaron que esta funcionalidad ya era suficientemente redundante en la capa de red y podía ser eliminada.

- *Opciones* en la cabecera estándar de IP ya no hay hueco para un campo de opciones. Sin embargo, no han desaparecido definitivamente, sino que el campo de opciones `podría ser una de las posibles siguientes cabeceras apuntadas desde la cabecera IPv6. Estos es, de igual forma que las cabeceras de los protocolos TCP y UDP pueden ser la siguiente cabecera

dentro del paquete IP, lo pueden ser también las opciones. La eliminación del campo de opciones de la cabecera proporciona una cabecera IP de longitud fija de 40 bytes.[4]

Figura 3. Datagrama IPv6



Fuente [2]

3.1.2 Características IPv6

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.

- Simplificación del formato del Header. Algunos campos del header IPv4 se quitan o se hacen opcionales

- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.

- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.

[4] REDES DE COMPUTADORES un enfoque descendente Basado en Internet. 2da edición. 2004. PEARSON Addison Wesley

- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.

- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.

- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además, el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.

- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.

- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.

- Calidad de servicio (QoS) y clase de servicio (CoS).

- Capacidades de autenticación y privacidad.[5]

[5] Características del protocolo de internet 6 [dia 19 de junio 2010, hora 2:30pm] página en internet [http://www.rau.edu.uy/ipv6/queesipv6.htm#10]

3.1.3 Definición de dirección en IPv6

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Dichas direcciones se clasifican en tres tipos:

- **Unicast:** Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

- ***Anycast*:** Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera "cae".

- ***Multicast*:** Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).[6]

3.1.4 Transición de IPv4 a IPv6

¿Cómo se realizará la transición de la Internet pública, basada en IPv4, a IPv6? El problema está en que mientras que los sistemas capaces con IPv6 pueden ser compatibles hacia atrás, es decir, pueden enviar, rutar y recibir datagramas IPv4,

[6] RFC2373, Arquitectura de Direccionamiento en IPv6
www.ietf.org/rfc/rfc3675.txt

los sistemas ya montados que funcionan con IPv4 no son capaces de manejar los datagramas IPv6. Hay varias opciones posibles.

Una opción podría ser declarar un día señalado: un momento y una fecha concreta en la que todas las maquinas de internet se apagarían y se actualizarían de IPv4 a IPv6. La última gran transición tecnológica (de NCP a TCP para el servicio de transporte fiable) ocurrió hace casi 20 años. [2]

Incluso entonces cuando la Internet era pequeña y aun era administrada por un reducido número de sabios, se vio que la idea del día señalado no era posible. Un día señalado que involucrara cientos de millones de màquinas y millones de administradores de red y de usuarios sería incluso más impensable hoy en día.

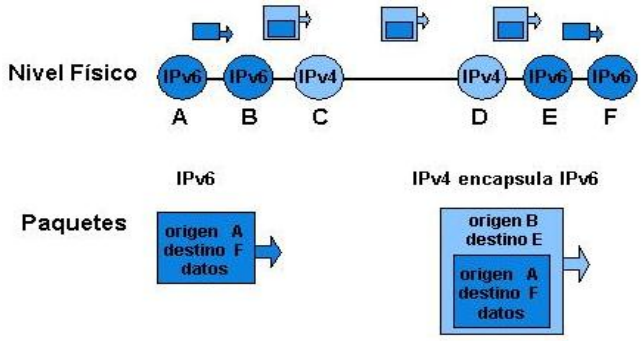
En RFC 2893 describe dos aproximaciones (que pueden usarse conjunta o aisladamente) para una integración gradual de los host y los routers IPv6 en un mundo IPv4 (con la meta a largo plazo, por supuesto, de efectuar la transición de todos los nodos de IPv4 a IPv6).

Probablemente la forma más directa de introducir los nodos capaces con IPv6 es una aproximación de **PILA DUAL**, en la que los nodos IPv6 también disponen de una implementación completa de IPv4. Tal nodo, denominado nodo IPv6/IPv4 en RFC 2893, tiene la capacidad de enviar y recibir tanto datagrama IPv4 como IPv6. Al interoperar con un nodo IPv4, el nodo IPv6/IPv4 usara datagramas IPv4; al interoperar con un nodo IPv6 podrá usar IPv6. Los nodos IPv6/IPv4 usarán datagramas IPv4; al interoperar con un nodo IPv6 podrá usar IPv6. Los nodos IPv6/IPv4 deben poseer tanto direcciones IPv6 como IPv4, además, deberán ser capaces de determinar si otro nodo es IPv6 o IPv4.

En la aproximación de pila dual, si tanto el emisor como el receptor son solo capaces con IPv4, deberá utilizarse un datagrama IPv4, en consecuencia, sería posible que dos nodos capaces con IPv6 acabaran, en esencia, enviándose uno a otro datagrama IPv4. Esto se refleja en la figura 4 suponga que el nodo A es

capaz con el IPv6 y desea enviar un datagrama al nodo F, que también es útil con IPv6. Los nodos AYB pueden intercambiar un datagrama IPv6. Sin embargo, el nodo B debe crear un datagrama IPv4 para enviárselo a C. Ciertamente, el campo de datos de datagrama IPv6 puede copiarse en el campo de datos del datagrama IPv4, y efectuarse la correspondencia apropiada entre direcciones. Sin embargo, al efectuar la conversión de IPv6 a IPv4, habrá campos específicos de IPv6 en el datagrama IPv6 (Por ejemplo, el campo de identificador de flujo) que no tienen contrapartida en IPv4. La información de estos campos se perderá. Así, incluso aunque E YF puedan intercambiar datagramas IPv6, los datagramas IPv4 que lleguen a E desde D no contendrán todos los campos que se enviaron inicialmente en el datagrama IPv6 desde A. [2]

Figura 4. Pila Dual

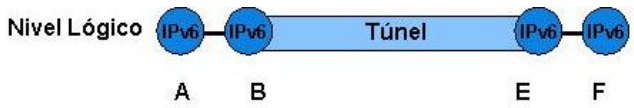


FUENTE: [2]

En RFC 2893 también se nombra una alternativa a la aproximación de pila dual conocida como **tunelizacion** *(tunneling).* La tunelizacion puede resolver el problema indicado anteriormente, permitiendo por ejemplo que E reciba el datagrama IPv6 originado por A. La idea básica que está detrás de la tunelizacion es al siguiente. Suponga que dos nodos IPv6 (por ejemplo, B y E en la figura 4) desean interoperar usando datagramas IPv6, pero están conectados uno a otro mediante routers IPv4. Por tanto los routers IPv4 que intervienen entre los routers IPv6 forman un **túnel**, como se muestra en la figura 5. Con la tunelizacion, el nodo IPv6 del lado emisor del túnel (por ejemplo B) encapsula el datagrama IPv6

completo en el campo de datos de un datagrama IPv4. Este datagrama IPv4 se remite entonces al nodo IPv6 del lado del receptor en el túnel (por ejemplo E), y se envía al primer nodo del túnel (por ejemplo C). Los routers IPv4 que intervienen en el túnel enrutan este datagrama IPv4 entre ellos, de la misma forma en que harían con cualquier otro datagrama, completamente inconscientes de que el datagrama IPv4 contiene un datagrama IPv6 completo. El nodo IPv6 del lado del receptor del túnel recibirá finalmente el datagrama IPv4 (es el destino del datagrama), determinará que el datagrama IPv4 contiene un datagrama IPv6, extraerá dicho datagrama IPv6, y entonces rutará el datagrama IPv6 exactamente como si hubiera recibido el datagrama IPv6 directamente de un vecino IPv6.[2]

Figura 5. Tunelizacion



FUENTE: [2]

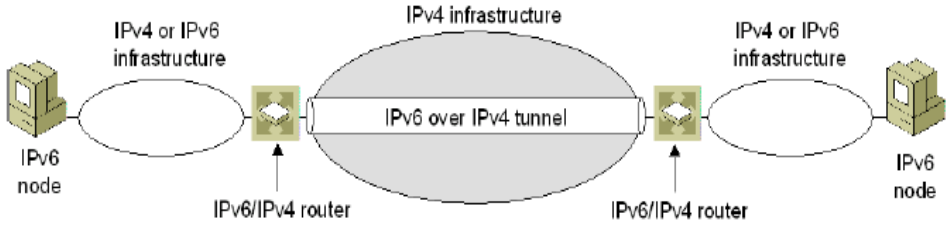
3.1.4.1 Ruteador a ruteador

En la configuración de túnel de ruteador a ruteador, dos ruteadores IPv6/IPv4 conectan dos infraestructuras IPv4 o UPv6 sobre una infraestructura IPv4. Los puntos finales del túnel expanden un enlace lógico en el camino entre el origen y el destino.

El túnel IPv6 sobre IPv4 ente los dos ruteadores actúan como un salto simple. Las rutas entre cada infraestructura IPv4 o IPv6 apuntan a los ruteadores IPv6/IPv4 en las orillas.

Para cada ruteador IPv6/IPV4, hay una interfaz del túnel que representa el túnel IPv6 sobre IPv4 y enruta el uso de la interfaz del túnel como se puede ver en la figura 6.

Figura 6. Túnel Ruteador a Ruteador



FUENTE: [5]

3.1.4.2 Equipo a ruteador y ruteador a equipo

En la configuración equipo a ruteador, un nodo IPv6/IPv4 que reside dentro de una infraestructura IPv4 crea un túnel IPv6 sobre IPv4 para alcanzar un ruteador IPv6/IPv4.

Los puntos finales del túnel expanden el primer segmento de la ruta entre los nodos origen y destino. El túnel IPv6 sobre IPv4 entre el nodo IPv6/IPv4 y el ruteador IPv6/IPv4 actúa como un solo salto.

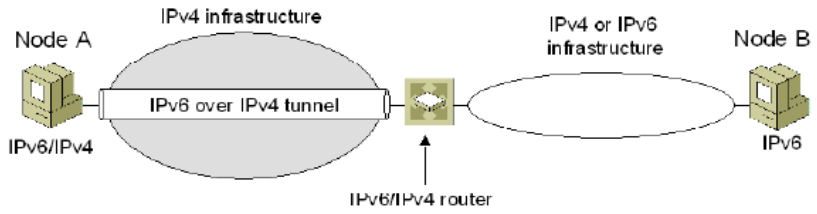
En el nodo IPv6/IPv4, se crea una interfaz del túnel que representa el túnel IPv6 sobre IPv4 y una ruta se añade usando la interfaz del túnel.

El nodo IPv6/IPv4 envía por el túnel el paquete IPv6 basado en la ruta coincidente, la interfaz del túnel y la dirección de siguiente salto del ruteador IPv4/IPv6.

IPv4 a través de una infraestructura IPv4 para alcanzar un nodo IPv6/IPv4, los puntos finales del túnel expanden el segmento final del camino entre el nodo origen y el nodo destino y el túnel IPv6 sobre IPv4 entre ruteador IPv6/IPv4 y el nodo IPv6/IPv4 actúa como un solo salto.

El ruteador IPv6/IPv4, se crea una interfaz de túnel que representa el túnel IPv6 sobre IPv4 y se añade una ruta utilizando la interfaz del tunal, el ruteador IPv6/IPv4 envía por el túnel el paquete IPv6 basado en la ruta de la subred que coincide y la dirección destino del nodo IPv6 como se pude apreciar en la figura 7.

Figura 7. Túneles Equipo a Ruteador y ruteador a Equipo



FUENTE: [5]

3.1.4.3 Equipo a Equipo

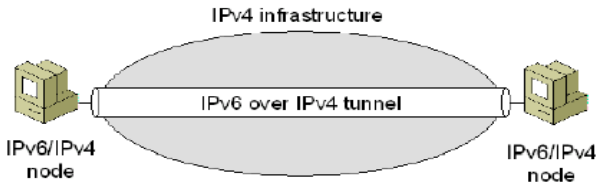
En la configuración de túnel de equipo a equipo, un nodo IPv6/IPv4 que reside en una infraestructura IPv4 crea un túnel IPv6 sobre IPv4 para alcanzar otro nodo IPV6/IPv4 que reside dentro de la misma infraestructura de IPv4. Los puntos finales del túnel expanden todo el camino entre el nodo origen y el destino, el túnel IPv6 sobre IPv4 entre los nodos IPv6/IPv4 actúan como una solo salto.

En cada nodo IPv6IPv4, se crea una interfaz que representa el túnel IPv6 sobre IPv4. La lógica definida por la infraestructura IPv4.

Basada en la interfaz que envía, la ruta opcional y la dirección destino, el host que envía, manda por el túnel el trafico IPv6 a su destino como se puede apreciar en la figura 8.[7]

[7] TEORIA Y METODOS DE TRANSICION IPv4 e IPv6
http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

Figura 8. Túneles Equipo a Equipo



FUENTE: [5]

3.1.4.4 6TO4

6to4 es una asignación de direcciones y tecnologías de túneles automáticos de ruteador a ruteador que se utiliza para proveer conectividad “unicast” entre sitios IPv6 y equipos a través de Internet IPv4. 6to4 utiliza el prefijo de direccionamiento global:

2002:wwxx:yyzz::/48

En el cual WWXX: YYZZ es la representación hexadecimal de una dirección IPv4 pública (W.X.Y.Z) asignada a un sitio o equipo. La dirección completa 6to4 es:

2002: WWXX: YYZZ: subnetID: InterfaceID

6TO4 se describe en RFC 3056, donde tiene los siguientes términos:

- Host 6to4. Cualquier host IPv6 que se configura con por lo menos una dirección 6to4 (una dirección global con el prefijo 2002::/16). Los host 6to4 no requieren ninguna configuración manual y crean direcciones 6to4 usando mecanismos de autoconfiguración de direcciones estándar.
- Ruteador 6to4. Un ruteador IPv6/IPv4 que soporta el uso de interfaces de túnel 6to4 y es usada típicamente para reenviar tráfico de direcciones 6to4 entre los hosts 6to4, dentro de un site u otros ruteadores 6to4. Los enrutadores 6to4 requieren procesamiento adicional lógico para el correcto

encapsulado y desencapsulado y pueden requerir configuración manual adicional.

Dentro de un site, los ruteadores IPv6 locales promocionan prefijos 2002:WWXX:YYZZ:SubnetID::/64 para que los hosts puedan crear una dirección 6to4 autoconfigurado y rutas de prefijo de 64 bits que se usan para entregar tráfico entre hosts 6to4 dentro del site.

Los hosts en las redes individuales son configurados automáticamente con ruta de subred de 64 bits para entregar directa a vecinos y una de default con la dirección de siguiente salto de ruteador que hace la promoción, todo el tràfico IPv6 que no coincide con un prefijo de 64 bits usado por una de las subredes dentro del site se reenvían a un ruteador 6to4 en la frontera del site.

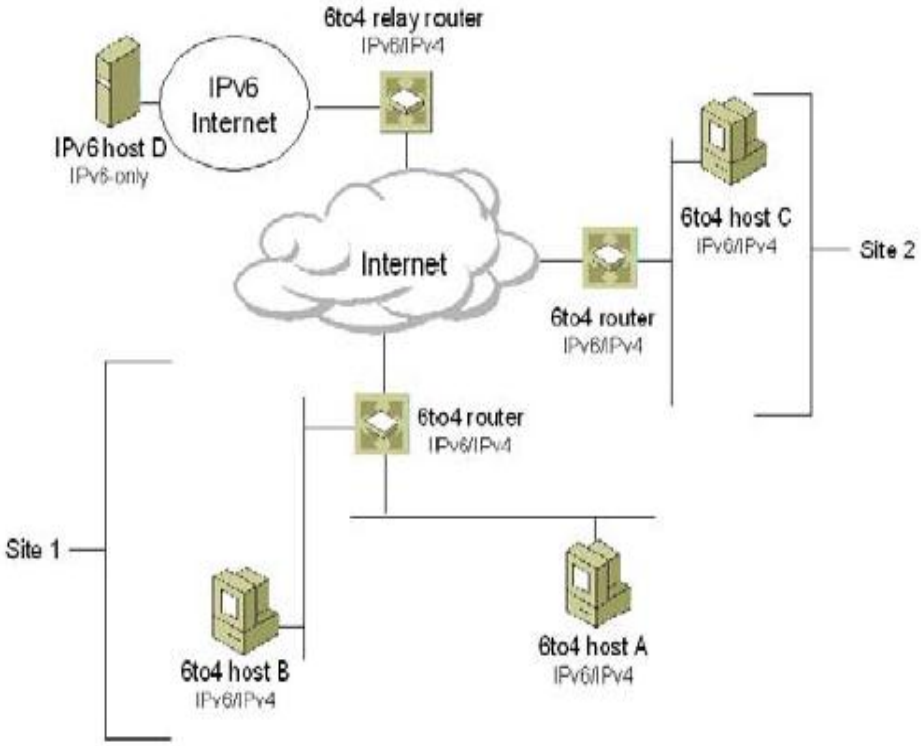
El ruteador 6to4 en la frontera del site, tiene una ruta 220.:/16 la cual es usada para reenviar tráfico para otros sitios 6to4 y la ruta de default (::/0) que es usada para reenviar tráfico para un ruteador 6to4 de realy.

En la figura 9, los equipos pueden comunicarse entre ellos debido a la ruta de default que utiliza la dirección del siguiente salto del ruteador 6to4 en el sitio1.

Cuando el host A se comunica con el Host C en otro site, el host A envía el tráfico al ruteador 6to4 del site 1 como un paquete IPv6, el ruteador 6to4 en el site 1 que usa la interfaz del túnel 6to4 y la ruta 2002::/16 en su tabla de ruteo, encapsula el paquete con un encabezado IPv4 y lo envía por el túnel al ruteador 6to4 en el site 2.

Cuando el ruteador 6to4 en el site 2 recibe el paquete por el túnel, quita el encabezado IPv4 y usando el prefijo de ruta de 64 bits en su tabla de ruteo reenvía el paquete a host C.[5]

Figura 9. Túnel 6TO4



FUENTE: [5]

4. CALIDAD DE SERVICIO

4.1 GENERALIDADES

La *Internet* actual es una red que ofrece un servicio de tipo *Best-Effort*, esto quiere decir, un servicio en el cual la red tratará de hacer su mejor esfuerzo para entregar los paquetes que recibe, pero la red no se compromete a garantizar la entrega de dichos datos. Estos paquetes podrían no llegar al destino por múltiples razones tales como la congestión, daños en enlaces entre *Encaminadores*, etc. Además, *Internet* no permite garantizar otros aspectos como el retardo de los paquetes y la reserva de ancho de banda para ciertas aplicaciones. Sin embargo, en la actualidad han surgido nuevas aplicaciones de tiempo real tales como vídeo-conferencia, o la transmisión de voz, las cuales requieren que la red que las soporta les garantice un mínimo de recursos para operar efectivamente. Además, *Internet* debe soportar diferentes tipos de aplicaciones que tienen diferentes tipos de requisitos. Los requisitos de servicio son específicos según las aplicaciones. Por ejemplo, un programa de audio sería sensible a un retardo de ida y vuelta; Una aplicación de transferencia de archivos es más sensible a la tasa de transmisión promedio o a la cantidad total de tiempo necesaria para transferir los datos.

4.2 PARÁMETROS DE CALIDAD DE SERVICIO

Las aplicaciones tradicionales, como correo electrónico, *Web, FTP*, etc. son transportadas por *Internet* actual con una clase de servicio muy pobre y denominada *Best Effort.* Con la aparición de nuevas aplicaciones de tiempo real es necesario mejorar la calidad de servicio. Una primera forma de enfocar la *QoS* es desde el punto de vista *cualitativo*; es decir, saber como un usuario final de una aplicación percibe la red. Dicho de otra manera, por la satisfacción que siente un usuario al finalizar una sesión en la red. El otro enfoque es desde el punto de vista *cuantitativo*, de aquellos parámetros que están relacionados directamente con la

mejora de la calidad de servicio y que al ser mejorados la red puede ofrecer una mejor calidad de servicio para aplicaciones que hoy en día son de gran importancia; videoconferencia, telefonía, control. Estos parámetros son: el ancho de banda, el retardo, la variación del retardo o *jitter* y la sensibilidad. Este tipo de parámetros son los que estudiaremos en este trabajo. A continuación se explicará cada uno de ellos.[8]

4.2.1 ***Ancho de Banda Mínimo***: Es la mínima cantidad del ancho de banda requerida por el flujo de una aplicación. Es necesario especificar el intervalo de tiempo para la medición del ancho de banda ya que diferentes intervalos de medición pueden producir diferentes resultados.

4.2.2 ***Retardo (delay):*** El retardo requerido puede ser especificado como el promedio de los retardos (*Retardo Medio*) o por el retardo del peor caso. El retardo que un paquete experimenta tiene tres componentes: retardo de propagación, retardo de transmisión y retardo de procesamiento. El retardo de propagación es limitado por la velocidad de la luz, y al mismo tiempo es una función de la distancia. El retardo de transmisión es el tiempo que tarda en enviarse un paquete en un enlace y depende de la longitud del paquete y de la velocidad del enlace; finalmente, el retardo de procesamiento es el tiempo de espera que experimenta un paquete en las colas de los *Encaminadores*.

4.2.3 ***Variación de Retardo (Delay Jitter)*****:** Este parámetro especifica la máxima diferencia entre el más largo y el más corto retardo que un paquete experimenta. En cualquier caso, la variación de retardo no debería ser más larga que el retardo del peor caso ni tampoco que el retardo de procesamiento.

[8] CALIDAD DE SERVICIO MULTICAPA EN UNA RED *IP* BASADA EN *WIMAX, Tesis de pregrado de Julieth katherin Ariza Olarte y Sergio Manuel Racini Bueno; Pagina 9*

4.2.4 *Tasa de Pérdidas* (*Loss Rate*): Es el cociente resultante entre los paquetes perdidos y el total de los paquetes transmitidos. La pérdida de paquetes en una *Internet* se debe usualmente a la congestión, y tales pérdidas pueden ser prevenidas mediante la asignación de suficiente ancho de banda y suficiente almacenamiento intermedio (*Buffers*) para el flujo de tráfico.

A la capacidad de una red para asegurar una cantidad de recursos y diferenciar servicios se le conoce como *Calidad de Servicio* (*QoS, Quality of Service*). Para que *Internet* tenga esta capacidad se han desarrollado dos soluciones básicas con diferentes formas de atacar el problema. La primera de ellas se conoce como *Arquitectura de Servicios Integrados* (*IntServ*) y la segunda se denomina *Arquitectura de Servicios Diferenciados* (*DiffServ*). [9]

4.3 Planificación de Paquetes

El *Planificador de Paquetes* es el responsable de asegurar la asignación de recursos a flujos individuales y decide qué paquetes deberían tomar los recursos. Un planificador puede verse como un despachador ya que mantiene información de cuántos paquetes ha enviado cada flujo y los compara con la cantidad de recursos que este ha reservado. Los paquetes de un flujo son enviados sólo cuando no se han usado todos los recursos reservados por este.

4.3.1 Requisitos Básicos de un Planificador

Los requisitos básicos de un planificador pueden resumirse en tres aspectos: Aislamiento y distribución de los paquetes, Límites de retardo de los paquetes y Asignación del ancho de banda. Estos aspectos se detallan a continuación.

[9] Contribución al soporte de Calidad del Servicio en Redes Móviles
http://www.tdr.cesca.es/TESIS_UPC/AVAILABLE/TDX-0319108-131609/01_padillaAguilar.pdf

4.3.1.1 *Aislamiento y Distribución*

El propósito de un planificador es permitir compartir un recurso común de forma controlada. En este ambiente hay dos aspectos importantes a tener en cuenta. El primero es el *Aislamiento de Flujos*, es decir, el grado de independencia entre los flujos que conlleva a que las alteraciones de un flujo no produzcan alteraciones a otros flujos.

El caso extremo de la independencia sería el de la conmutación de circuitos. Sin embargo, en este caso los recursos reservados se sub-utilizan para el caso de la transmisión de datos. El segundo aspecto es la *Distribución de Recursos*. Esto se refiere al manejo eficiente de un recurso, lo que se logra con la multiplexación estadística usada en conmutación de paquetes. Por tanto, hay un compromiso entre estos dos aspectos. Una solución que logra un balance es la que se conoce como *Algoritmo de Distribución Justa* (*Fair-Queuing*).

4.3.1.2 *Límites de retardo*

Hay dos tipos de límites de retardo de los paquetes. Por una parte están los límites *Determinísticos* que requieren fuertes garantías de reservas. Un ejemplo de este tipo es el retardo del peor caso en *IntServ*. Por otro lado, están los límites *Estadísticos* que permiten *Multiplexación Estadística*. Ejemplos de este tipo de límites son los retardos por un tiempo máximo debido al crecimiento de las colas y el valor medio de retardo de los paquetes.

4.3.1.3 *Asignación de ancho de banda*

Cuando no hay suficientes recursos para satisfacer las demandas de tráfico, debe asignarse de forma justa el ancho de banda para todos los flujos en competencia. Una política de distribución justa de recursos (*Criterio de Justicia*) que ha sido ampliamente considerada en la literatura es llamada *Max-Min Fair Sharing*.

4.3.2 Algoritmos de Planificación tipo Fair-Queuing

Los algoritmos de planificación pueden ser clasificados en general en 3 categorías:

Algoritmos de Distribución Justa (*Fair Queuing*), *Algoritmos Basados en Plazos* (*Deadline Based*) y *Algoritmos Basados en Tasas* (*Rate Based*). Por ser de nuestro especial interés debido a que es el tipo usado en el estándar de *Servicios Integrados*, nos enfocaremos en los algoritmos de tipo *Fair-Queuing*. En la aproximación *Fair-Queuing*, el ancho de banda asignado a un flujo es representado por un número real, a menudo denominado *Peso*. Estos algoritmos tratan de asignar un *Ancho de Banda* (*BW*) proporcional a los flujos activos o represados con base en sus pesos. Si un flujo no consume todo el *BW* asignado, el *BW* restante es asignado a flujos represados en proporción a sus pesos. De esta forma, se le garantiza a un flujo que puede usar su *BW* asignado y podría usar más. Además, se puede proveer un límite de retardo extremo a extremo (*End-to-End ó E2E*). Por estas razones, este tipo de algoritmos se usan en *IntServ*.

El más conocido de los algoritmos de planificación de tipo *Fair-Queuing* es el *WFQ* (*Weighted Fair Queuing*). *WFQ* fue propuesto hace más de 10 años y soporta la asignación de *BW* y límites de retardo. Este algoritmo tiene variantes con diferentes compromisos entre complejidad y precisión y ha sido implementado ampliamente en *Encaminadores* para soportar *QoS*. *WFQ* es descrito a menudo como un modelo de fluidos. En el modelo de fluidos se asume que el tráfico es infinitamente divisible y que un nodo puede servir múltiples flujos simultáneamente. Sin embargo, en una red real los paquetes son procesados uno a la vez y por tanto, el tamaño del paquete afecta el sistema de colas. Por ser un algoritmo construido para funcionar en una red real, *WFQ* trata de adaptar el modelo de fluidos a un modelo paquetizado.[7]

4.3.3 MDRR

Una variación de la DRR que se enfoca en la minimización del retardo para unos ciertos flujos de tráfico. Esto es útil, por ejemplo, en el manejo de paquetes de VoIP. Aunque los flujos VoIP necesitan tanto garantías de ancho de banda, como garantías de retardo de los paquetes, podemos pensar en un acercamiento alternativo de proporcionar una garantía de ancho de banda con retrasos mínimos (minimizar la demora). El esquema MDRR se centra en la forma de minimizar los retrasos ó demoras con base en el esquema de planificación DRR. Por ejemplo, puede hacerse una modificación asignando prioridades a las colas de espera, lo que sirve como una planificación de prioridades para diferentes colas. Por ejemplo, se podría definir una cola con ultra alta prioridad, la cual siempre obtendrá prioridad si tiene paquetes para enviar y no se le limitara el tamaño del Quantum. La palabra "modificación" en MDRR no necesariamente tiene esta aproximación; se pueden hacer diferentes modificaciones. Vale la pena señalar que la mayoría de los vendedores de routers en la actualidad implementan alguna forma de cola de espera MDRR.[10]

[10] Network Routing. Algorithms, Protocols, and Architectures. DEEPANKAR MEDHI, KARTHIKEYAN RAMASAMY; Pagina 10

5. MOVILIDAD EN IP

Actualmente, las direcciones en *Internet* son utilizadas entre otros aspectos para la identificación del sistema final, además *TCP* usa las direcciones *IP* para seguir la pista del estado de la sesión interna entre los dos extremos. Las direcciones también se usan para encontrar la ruta entre los dos extremos (la ruta no es la misma en las dos direcciones ya que depende de la dirección del destino y de la congestión de la red). En este punto aparece un gran dilema: Un ordenador necesita una dirección *IP* estable para ser identificable en forma estable por otros ordenadores de *Internet*, sin embargo, si la dirección *IP* es estable, el encaminamiento hacia el ordenador móvil es estable y los *Datagramas* siempre irán al mismo sitio. Por tanto no hay movilidad. Para dar solución a este problema han surgido varias propuestas que buscan solucionar el la movilidad de diferentes maneras y en diferentes situaciones. Así, existen propuestas que solucionan la movilidad en entornos denominados de *macro-movilidad*, es decir, cuando se cambia de una *Red de Acceso* a otra (la más aceptada hasta el momento se denomina *IP Móvil* ó *Mobile IP.* En general, los protocolos de *micro-movilidad* buscan disminuir la cantidad de señalización requerida por los protocolos de *macro-movilidad* cuando los *Encaminadores de Acceso* se encuentran muy cerca entre sí. [7]

5.1 MOVILIDAD EN IPV4

Mobile IPv4 considera dos tipos de redes conectadas a *Internet*:

- *Home Network:* (*Red Doméstica*) Esta es una red en la que se encuentra matriculado un ordenador móvil.
- *Visited Network:* (*Red Visitada*) Es una red a la que se conecta un ordenador móvil cuando no se encuentra en su *Red Doméstica* y le permite al ordenador móvil conectarse a *Internet* como un huésped.

La solución suministrada con *IP Móvil,* en sus dos versiones, consiste en que los ordenadores móviles siempre se identifican por una dirección fija denominada *Home Address* (*Dirección Doméstica*) sin tener en cuenta su punto actual de acceso a *Internet*. Mientras esté fuera de su *Red Doméstica,* cada ordenador móvil tiene una dirección adicional que identifica su localización actual: la *CoA* (*Care of Address*) *ó Dirección a Cargo* (también se conoce como *Dirección Temporal*). Así, los mensajes que llegan a la *Dirección Doméstica* original son re-enviados mediante un túnel a la *CoA*.[7]

Ahora se describirán las entidades que intervienen en *Mobile IPv4* (ver Figura 9):

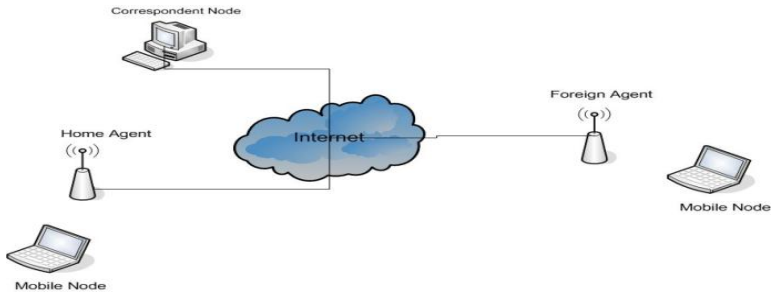
- *Mobile Node (MN):* Es un ordenador móvil que cambia su punto de conexión de una red o subred a otra. Mantiene una dirección *IP* constante. En este documento también se le llama *Nodo Móvil*.

- *Correspondent Node (CN):* Es el ordenador que se comunica con el *MN* a través de *Internet* (es el otro extremo de la comunicación). Puede ser fijo o móvil. En este documento también se le llama *Nodo Correspondiente*.

- *Home Agent (HA):* También se conoce como *Agente Propio*. Es un *Encaminador* ubicado en la *Red Doméstica*. Todo *Datagrama* que vaya hacia el *Nodo Móvil* debe pasar por el *Agente Propio* y este lo reenvía al *MN*.

- *Foreign Agent (FA):* Conocido también como *Agente Visitado*. Es un *Encaminador* ubicado en la *Visited Network*. Este colabora con el *Home Agent* para entregar los *Datagramas* a un nodo móvil que se encuentra conectado a la *Red Visitada.*

Figura 10. Movilidad IPv4



FUENTE [7]

5.2 MOVILIDAD EN IPV6

Mobile IPv6 es muy similar a *Mobile IPv4***,** la diferencia más grande radica en que, normalmente se realiza *Optimización de la ruta* en lugar del *Triángulo de Encaminamiento* para el encaminamiento de los paquetes.

5.2.1 *Mensajes de Mobile IPv6*

Mobile IPv6 requiere el intercambio de información adicional. Los nuevos mensajes usados en *Mobile IPv6* son definidos como *Opciones de Destino* de *IPv6*. Por consiguiente, la información llevada sólo será examinada por el nodo de destino del paquete. Las nuevas *Opciones de Destino* definidas en *Mobile IPv6* son:

- *Actualización de Vinculación (BU, Binding Update)*: Un *MN* informa a su *HA* o a cualquier *CN* sobre su *CoA* actual usando la opción de *Actualización de Vinculación*.
- *Confirmación de Vinculación (BAck)*: Se usa para reconocer la recepción de una *actualización de Vinculación* (si el reconocimiento fuera solicitado).
- *Solicitud de Vinculación (BR, Binding Request)*: Cualquier nodo, para solicitar a un *MN* enviar un *BU* con la actual *CoA*, usa la opción de *Solicitud de Vinculación*.

- *Dirección Doméstica (Home Address)*: La opción de la *Dirección Doméstica* se usa en un paquete enviado por un *MN* para informar al receptor de este paquete sobre la *Dirección Doméstica* del *Nodo Móvil*.[7]

5.2.2 Estructuras de datos usadas en MIPv6

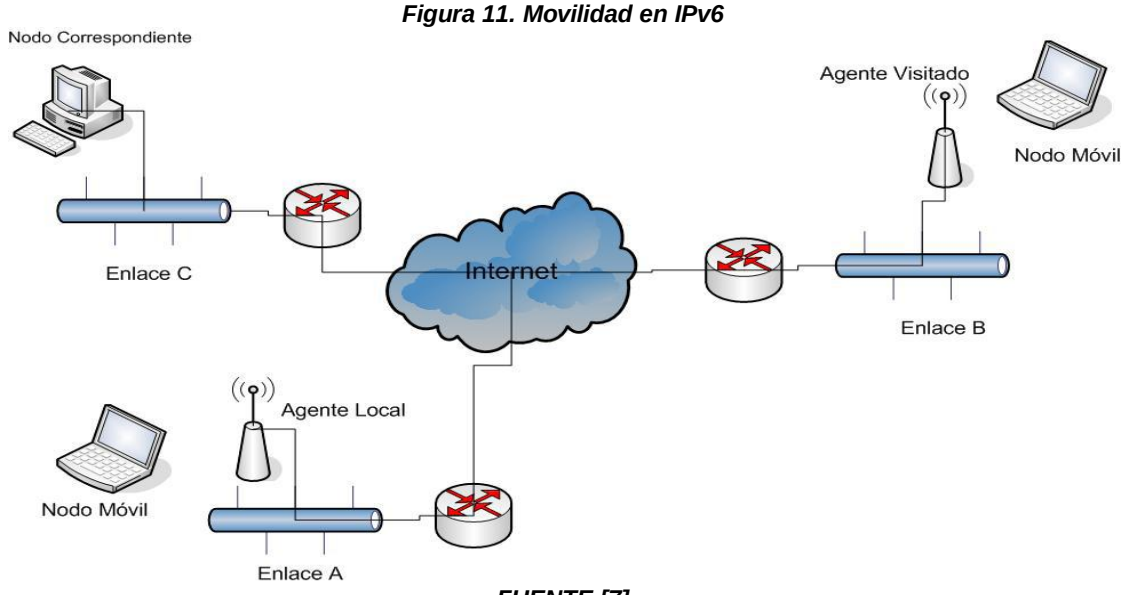
La especificación de *Mobile IPv6* describe las siguientes tres estructuras de datos: *Caché de Vinculaciones (Bindings Cache)*: Cada nodo tiene un *Caché de Vinculaciones* que se usa para almacenar las *Vinculaciones* (*Bindings*) de otros nodos.
Si un nodo recibe un *BU*, agregará esta *Vinculación* a su *Caché de Vinculaciones*. Así mismo, cuando quiera enviar un paquete, se busca una entrada en el *Caché de Vinculaciones*. En caso de que haya una entrada, el paquete se envía a la *CoA* del *Nodo Móvil* respectivo usando una *Cabecera de Encaminamiento* de *IPv6*. *Lista de BU's*: Cada *Nodo Móvil* tiene una *Lista de BU's* que se usa para guardar la información sobre cada *Actualización de Vinculación* enviada por él y para las cuales el tiempo de vida no ha expirado aún. Esta lista contiene todos los *BUs* enviados a su *HA* y a cualquier *Nodo Correspondiente* (móvil o estacionario), es decir los nodos que se están comunicando o se han comunicado hace corto tiempo con el *MN*. *Lista de HA's*: Para cada *Enlace Doméstico* (*Home Link*), es decir, una *Red Doméstica*, un nodo que sirve como *HA* genera una lista que contiene la información sobre todos los otros *HA*'s en esta red. La información en esta lista es aprendida de los *Mensajes Multicast de Anuncio* de los *Encaminadores*, los cuales son enviados desde todos los *HA*. La información acerca de los otros *Agentes Domésticos* es usada por el *DHADM* (*Dynamic Home Agent Discovery Mechanism*).[7]

5.2.3 Operación de Mobile IPv6

A continuación se explicarán los mecanismos de *Mobile IPv6*, para lo que se usará la Figura 10. La figura muestra tres enlaces y tres sistemas. En el *Enlace A (Red Doméstica)* reside un *Encaminador* que ofrece el servicio de *HA*. Este enlace es llamado también el *Enlace Doméstico* del *Nodo Móvil*. Este *Nodo Móvil* (*MN*) simplemente se mueve del *Enlace A* para unirse al *Enlace B (Red Visitada)*. Adicionalmente hay un *Nodo Correspondiente* sobre el *Enlace C* que puede ser móvil o estacionario. A continuación se detallarán los procedimientos de *Registro* y de *Envío de Datagramas* mediante el *Triángulo de Encaminamiento* y mediante la *Optimización de la Ruta*.

*Registro de un HA:*En cuanto un *Nodo Móvil* detecta que se ha movido de un *enlace* a otro, y ha descubierto un nuevo *encaminador*, el *MN* realiza una auto-configuración de la dirección y usa la nueva dirección asignada como su *CoA*. El prefijo de esta *CoA* es el prefijo de la *Red Visitada* en que se encuentra ahora el *Nodo Móvil;* todos los paquetes serán dirigidos ahora a esta *CoA* y localizarán el *MN* en el *Enlace* actual.[7]

Figura 11. Movilidad en IPv6



FUENTE [7]

El *MN* registra su *CoA* con su *HA* en el *Enlace Doméstico*. Por consiguiente el *MN* envía un paquete, que contiene una opción *BU,* a su *HA*. El *HA* registra este enlace y retorna un paquete con una opción de *Confirmación de Vinculación* (*BAck*) al *Nodo Móvil*. [7]

- *Triángulo de Encaminamiento:*

Una vez él *HA* haya introducido la *CoA* de un *MN* en su *Caché de Vinculaciones*, interceptará cualquier paquete enviado a la *Dirección Doméstica* del *Nodo Móvil*. Para ello, usa el procedimiento denominado *Proxy Neighbor Discovery* (*Descubrimiento de Vecinos*). Cada paquete interceptado es encapsulado a la *CoA* registrada del *MN* usando *Encapsulado de IPv6*.

En sentido contrario, cuando el *MN* envía los paquetes a cualquier otro nodo, envía los paquetes directamente al destino. El *MN* pone en la *Dirección Origen* de este paquete la *CoA* e incluye una *Opción de Destino* de tipo *Dirección Doméstica*. Debido a que la *Dirección Doméstica* es estática (en contraste con la *CoA*), es posible que cada *Nodo Correspondiente* use transparentemente la *CoA*. Las capas superiores (incluso las aplicaciones) no consideran la *CoA*, ellas sólo utilizan la *Dirección Doméstica*.

Si un *MN* se comunica con un *Nodo Correspondiente* que está fuera de su *Red Doméstica*, los paquetes son enviados desde el *CN* al *HA*, luego desde el *HA* al *MN* y en sentido contrario directamente desde *MN* al *CN*. Este es el ya mencionado *Triángulo de Encaminamiento*. [7]

- *Optimización de la Ruta:*

Para evitar el problema del *Triángulo de Encaminamiento*, un *MN* puede enviar *BU*'s a cualquier *CN* (Móvil o estacionario). Esto permite a los *CNs* almacenar la *CoA* actual y enviar los paquetes directamente a un *MN*.

Cualquier *Host IPv6* que envía un paquete verifica primero su *Caché de Vinculaciones* para esta *Dirección de Destino*. Si hay una entrada, enviará el paquete al *MN* usando una *Cabecera de Encaminamiento* (en lugar de usar *Encapsulado de IPv6*). La ruta especificada por esta *Cabecera de Encaminamiento* tiene dos saltos. El primer salto es la *CoA* y el segundo salto es la *Dirección Doméstica* del *MN*. Esto produce que el paquete sea enviado directamente a la *CoA* del *MN*. El *MN* recibe este paquete y lo envía al próximo salto especificado en la *Cabecera de Encaminamiento*. El próximo y último salto es la *Dirección Doméstica* del *MN*, por consiguiente este paquete se absorbe en el *MN*.

Si el *Caché de Vinculaciones* no tiene ninguna entrada, este paquete será enviado normalmente. Entonces este paquete se envía a la red especificada y es recibido por el *Nodo de destino*. En caso de que el destino sea un *MN* que está en una *Red Visitada*, este paquete será interceptado por un *HA* y será encapsulado al *MN*. [7]

6. SEGURIDAD

Desde nuestro repaso de la arquitectura IPv6, recordemos que tanto el encabezado de extensión Authentification (AH) como Encryption (ESP) han sido definidos y son requeridos para una implementación completa de IPv6. Los encabezados Authentification y Encryption son parte del trabajo en curso en IP Security (Ipsec), que es direccionar aplicaciones para IPv4 e IPv6. Un archivo de los estándares Ipsec está disponible desde el *Virtual Private Networking Consortium.*

Las funciones de autentificación y cifrado (encryption) han sido separadas de tla manera que las implementaciones individuales pueden usar una o ambas de las funciones como sean necesitadas por las aplicaciones de capa más alta. Cifrado, por ejemplo, puede ser restringida para regulación gubernamental; así, solo la autentificación esta implementada en algunos casos.[9]

6.1. Arquitectura de Seguridad IP (IPSEC)

La meta de IP Security (Ipsec) es proveer seguridad basada en criptografía, interoperable para IPv4 e IPv6. Como estas funciones de seguridad son ofrecidas en las capa IP, la protección para tanto IP como cualquier capa más alta de protocolos es proveída. Ipsec habilita a un sistema seleccionar los protocolos de seguridad requeridos, determinar los algoritmos que serán usados para el servicio de seguridad, e implementar cualquier clave criptográfica que sea requerida para proveer estos servicios. Ipsec puede ser usado para proteger los caminos de comunicación entre 2 hosts, entre 2 gateways de seguridad o entre un host y un Gateway de seguridad.

La arquitectura de seguridad para IPv6 está definida en RFC 2401. Este documento incluye las siguientes definiciones base para varios sistemas y procesos:

- Control de acceso: El proceso de prevenir acceso no autorizado a un recurso de red.
- Autentificación: La verificación de identidad de la fuente reclamada de los datos (también conocido como autentificación del origen de los datos), mas la propiedad que un paquete IP individual no ha sido modificado (integridad sin conexión).
- Integridad: La propiedad de asegurar que los datos son transmitidos desde una fuente o destino sin modificación sin detectar. Integridad sin conexión es un servicio que detecta la modificación de un paquete IP individual, sin importar el orden del paquete en un stream de datos. Integridad anti-replay (o integridad de secuencial parcial) detecta la llegada de paquetes IP duplicados dentro de una ventana.
- Confidencialidad: La protección de los datos de acceso no autorizado.
- Cifrado: Un mecanismo para transformar los datos desde una forma inteligente (plaintext) a una forma no inteligente (ciphertext), así proveyendo confidencialidad.
- Índice de parámetros de seguridad (SPI): Un valor de 32 bits que es usado para distinguir entre diferentes asociaciones de seguridad (SAs) terminando en el mismo destino y usando el mismo protocolo IPSec.
- Asociación de Seguridad (SA): Una simple (unidireccional) conexión lógica. Creada para propósitos de seguridad. Tanto Authentification (AH) como Encryption (ESP) hacen uso de las asociaciones de seguridad (SAs).

  La Asociación de seguridad (SA) es una simple conexión lógica (de una vía) que provee servicios de seguridad a los Authentification (AH) o Encryption (ESP) pero no a ambos. Así, si tanto un Authentification (AH) como un ESP se les aplican el mismo stream de tráfico, 2 SA debe ser asignada. Además, sesiones de comunicaciones bidireccionales, autentificadas entre 2 hosts tendrán 2 SA en uso- uno en cada dirección. La Asociación de seguridad (SA) puede incluir: el algoritmo de autentificación, el modo del algoritmo y claves; el algoritmo de cifrado, el modo del algoritmo, y claves. Tiempo de

vida de la clave, o tiempo en que la clave debe ser cambiada, y así. Dos tipos de La Asociación de seguridad (SA) son definidos: modo de transporte y modo túnel.

- Gateway de seguridad: Un sistema que actúa como un sistema intermediario entre 2 redes. Los hosts o redes en el lado externo del Gateway de seguridad son vistos como sistemas no confiables (o menos confiables), mientras que los hosts o redes en el lado interno son vistos como sistemas confiables (o más confiables).
- Análisis de tráfico: El análisis del flujo de tráfico en la red para el propósito de deducir información que es útil para adversario. Ejemplos de este tipo de información con la frecuencia de transmisión, las identidades de las partes que conversan, tamaño de los paquetes, identificadores de flujos usados, y así.
- Subred Confiable: Una red que contiene hosts y routers que se confían entre sí para no comprometerse en ataques activos o pasivos, y que confían que el canal de comunicación subyacente (ejemple: Ethernet) no está siendo atacado.
- Asociación de Seguridad en Modo de Transporte: Una Asociación de seguridad (SA) entre 2 hosts, primariamente proveyendo seguridad para los protocolos de capa más alta.
- Asociación de Seguridad en Modo en Túnel: una Asociación de seguridad (SA) aplicada a un túnel de IP, primariamente proveyendo seguridad para un paquete en el túnel.[9]

Las siguientes secciones discuten las varias asociaciónes de seguridad (SA) que son posibles, mas la manera en que Authentification (AH) Y Encryption ESP son implementadas dentro de estas asociaciónes de seguridad (SA).

6.2 Asociaciones de Seguridad

La Asociación de Seguridad (SA) es una conexión lógica simple (o de una vía) que provee servicios de seguridad al tráfico que está siendo cargado sobre esa conexión. Estos servicios de Asociación de seguridad (SA) pueden ser proveídos a Authentification (AH) o Encryption (ESP) pero no a ambos. Si se desean un Authentification (AH) un Encryption ESP, dos Asociaciones de Seguridad SA son requeridas.

Dos tipos de asociaciónes de seguridad (SA) son definidos: modo de transporte y modo de túnel. El SA en modo de transporte existe entre dos hosts. Para el modo de transporte, el encabezado de protocolo de seguridad (AH O ESP) aparecería después del encabezado IP y otro encabezado de extensión opcionales, pero pueden aparecer antes o después del encabezado de destino, y antes de cualquier encabezado IP y protocolos de capa más alta. Cuando ESP es empleado en modo de transporte, la seguridad es proveida para solo los protocolos de capa más alta.

En modo de túnel la SA es aplicada al túnel, donde un extremo del tùnel es un Gateway de seguridad, el modo de túnel debe ser usado. Si los dos extremos del túnel son hosts, entonces el modo de túnel o de transporte puede ser usado. Para el modo de túnel, hay 2 encabezados IP: Un encabezado interno que especifica el destino para el proceso Ipsec, y un encabezado interno que especifica el destino del paquete. Cuando AH es empleado en modo de túnel, la seguridad es proveida por porciones del encabezado externo IP más todo el paquete de túnel interno. Cuando ESP es empleado en modo de túnel, la seguridad es proveida solo para el paquete de túnel interno.

Una asociación de seguridad individual usa solo un protocolo de seguridad: AH o ESP. Si la política de seguridad dicta habilidades que no son ejecutables con un solo protocolo de seguridad, múltiples SAs pueden ser usadas para esta implementación. El termino paquete de asociación de seguridad es aplicado a esa

condición. Las asociaciones de seguridad pueden ser combinadas en paquetes en 2 formas: Un trasporte adyacente o tunneling iterado al mismo paquete IPv6, sin usar tunneling. Múltiples niveles de protocolos de seguridad son implementados a través de tunneling, con cada uno de estos túneles terminando posiblemente en un endpoint. Con el modo de transporte, si tanto AH como ESP son usados, AH debe aparecer como el primer encabezado después de IPv6, seguido por ESP. Con esta secuencia, la autentificación es así aplicada a la salida cifrada de ESP. Con el modo de túnel, ordenes diferentes de AH y ESP son posibles, dependiendo de los requerimientos de seguridad.[9]

6.3 Autentificación

El Authentification Header (AH) provee integridad sin conexión, autentificación del origen de los datos y un servicio ante-replay opcional. AH está definido en RFC 2402. AH puede ser implementado en dos formas: modo de trasporte (entre hosts) y modo de túnel (entre hosts y gateways de seguridad, o entre 2hosts). AH es un protocolo apropiado para implementar cuando la confidencialidad no es requerida o no es permitida (por regulaciones gubernamentales, por ejemplo).

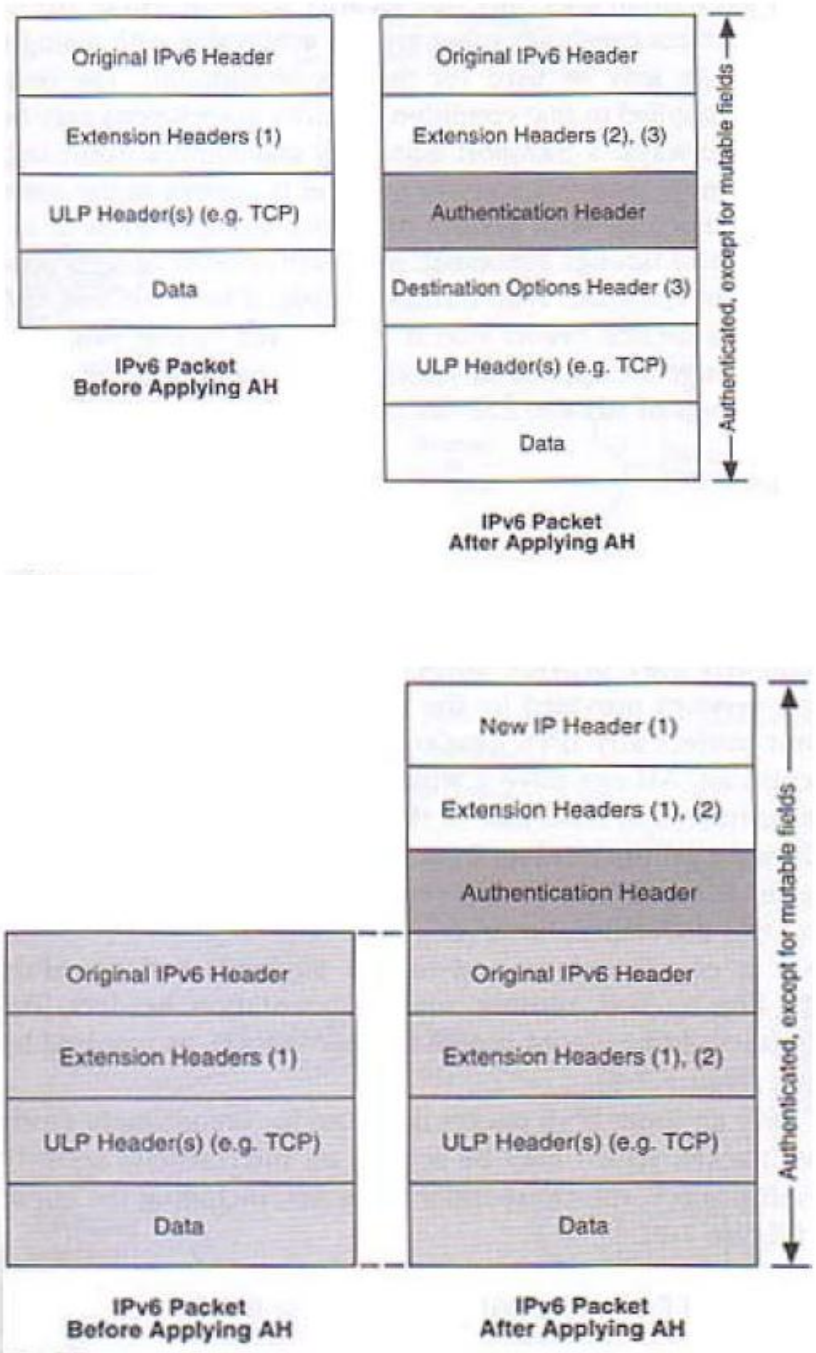
Note que tanto ESP como AH pueden proveer autentificación. La diferencia clave entre los servicios de autentificación proveídos por los 2 protocolos es el grado de cobertura. ESP no protege ningún campo del encabezado IPv6 a menos que esos campos estén encapsulados por ESP. En contraste, AH puede tener un rango de cobertura más amplia.

En modo de transporte, AH está considerado una carga útil de extremo a extremo, así que debe ser colocado después de los encabezado hop-by-hop, routing y fragmentación. El encabezado (o los encabezados) Destination Options puede ser colocado antes o después de AH, como lo requiera la implementación especifica.

El modo de túnel contiene tanto un paquete interno IPv6 (para el destino) como un paquete externo IPv6, que puede ser enviado a un Gateway de seguridad

intermedio. En modo de túnel, AH protege el paquete interno IP completo, incluyendo el encabezado del paquete interno IPv6.[9]

Figura 12. Autentificacion



FUENTE [9]

6.4 Encriptación

Encapsulated Security Payload (ESP) provee confidencialidad (cifrado), autentificación del origen de los datos, integridad sin conexión, servicio antireplay y confidencialidad de flujo de tráfico limitado (guardando contra análisis de tráfico). Tanto AH como ESP pueden ser usados para control de acceso, basado en los flujos de tráfico y distribución de claves en uso. El alcance de la autentificación ofrecido por ESP no es tan amplio como el proveído por AH. ESP está definido en RFC 2406.

En modo de transporte, ESP es considerado una carga útil de extremo a extremo, así que debe ser colocado después de los encabezado hop-by-hop, routing y fragmentation. El encabezado (o los encabezados) Destination Options pueden ser colocado antes o después de ESP. Sin embargo, como ESP protege solo los campos que van después del encabezado ESP, colocar el encabezado Destination Options después de ESP es deseable.

El modo túnel contiene tanto un paquete interno IPv6, para el destino, como un paquete externo IPv6, que puede ser enviado a un Gateway de seguridad intermedio. En modo de túnel, ESP protege el paquete interno IP completo, incluyendo en encabezado del paquete interno IPv6.[11]

[11] Nueva generación Protocolo de Internet, FACULTAD DE CIENCIA Y TECNOLOGIA ESCULA DE INFORMATICA, Trabajo de para optar el titulo de ingeniería sistema, 2004. http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf

7. OPNET MODELER

7.1 INTRODUCCIÓN A LOS SIMULADORES

Se define la simulación como una técnica que imita el comportamiento de un sistema del mundo real conforme evoluciona en el tiempo. Por lo tanto, se podrán analizar y observar diferentes características, sin la necesidad de acudir al sistema real. Surgen pues, de éste concepto, dos nuevas definiciones:

- **Modelo de simulación**: Se refiere al conjunto de hipótesis acerca del funcionamiento del sistema expresado como relaciones matemáticas y/o lógicas entre los elementos del sistema.

- **Proceso de simulación**: Es la ejecución del modelo a través del tiempo en un computador para generar los resultados del comportamiento del sistema.

En resumen, se puede decir que el modelo hace referencia a la representación del sistema real que se va a analizar, las condiciones de su funcionamiento, y las variables que emplea. En cambio, el proceso hace referencia a una ejecución concreta, con unos valores asociados a las variables que se pueden ajustar en el modelo, y que se realiza para obtener los resultados referidos a ciertos parámetros que especifican el comportamiento del sistema.
La simulación se limita a informar de cuál sería el comportamiento del sistema analizado en las condiciones que se indiquen para un proceso determinado.[10]

Otra definición muy importante corresponde a la de sistema. Un sistema es un conjunto de elementos que, actúan e interactúan para lograr algún fin.
Cuando se habla de *estado del sistema* se hace referencia al conjunto de variables necesarias para describir el estado del sistema en un determinado instante de tiempo. Entre todas estas variables se tienen que distinguir las entradas y las salidas. Las salidas están expresadas mediante valores numéricos.

Las entradas serán los valores numéricos que permitan iniciar la simulación y obtener las salidas. En estas entradas, se incluyen:

- **Las condiciones iniciales**: Valores que expresan el estado del sistema al principio de la simulación.

- **Datos determinísticos**: Valores conocidos necesarios para realizar los cálculos que producen las salidas.

- **Datos probabilísticos**: Cantidades cuyos valores son inciertos pero necesarios para obtener las salidas del sistema. Los valores específicos de estos datos pueden generarse a través de una distribución de probabilidad.

7.2 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.

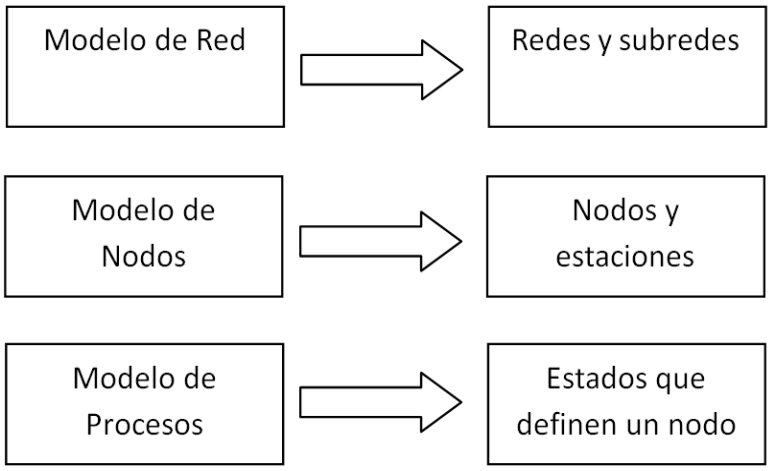
Actualmente es utilizado por grandes empresas de telecomunicaciones, por ejemplo para desarrollar proyectos gubernamentales y del ejército, etc.
Para más detalle se dispone de su página oficial *http: //www.opnet.com*, donde se puede encontrar toda la información referente a cómo descargar el software necesario, qué es OPNET, etc.[10]

7.2. Cómo funciona OPNET *Modeler*

Como se verá a continuación, OPNET es un simulador que posee una interfaz muy seductora para los usuarios. Esto es debido a que incluye varias librerías de modelos. El código fuente de estas librerías es accesible si se dispone de la versión OPNET *Modeler* y esto consigue que el programador se pueda familiarizar más rápidamente con toda la jerarquía interna del programa.

Para ser utilizado, primero el usuario tiene que comprender la jerarquía que se utiliza para poder plantear las simulaciones. Esta jerarquía de diseño se muestra en la figura 13.

Figura 13. Jerarquia en Opnet



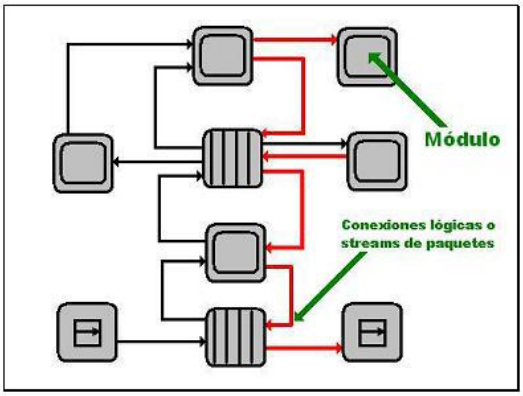
FUENTE [10]

Como podemos observar en la figura anterior, se tiene un modelo de red donde irán definidas las redes y subredes de la simulación. Seguidamente se dispone de un modelo de nodos donde se define la estructura interna de éstos y por último se tiene el modelo de procesos donde se definen los estados que definen un nodo.

En la correcta simulación de un proyecto se debe haber entendido los aspectos anteriores; puestos que de lo contrario la simulación saldría errónea y no serviría.

Como se ha mencionado con anterioridad, se posee un modelo de nodos. Este modelo de nodos funciona como se muestra la figura 14.[10]

Figura 14. Funcionamiento



FUENTE [10]

Un nodo puede tener en su interior varios módulos. Éstos módulos tienen una función definida en su interior, así, un módulo llamado *receptor* tendrá la función de recibir los paquetes de otro. Para modificar los módulos de la simulación se necesita tener el *node editor,* que se puede encontrar en el OPNET *Modeler.*

Los módulos que ofrece el *node editor* son descritos en la tabla 1.

Todos estos módulos se relacionan directamente con los procesos mediante la opción *Process Model* en su opción *edit attributes.* Para realizar lo anterior, se da doble clic encima de cualquier nodo del escenario de simulación para abrir el *Node Model.* Una vez en el *Node Model,* se da clic derecho encima del módulo a modificar y se selecciona *edit attributes.*

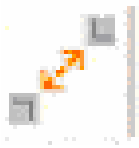
Por otra parte, las conexiones lógicas que ofrece el *node editor* son descritas en la tabla 2.

Tabla 1. Módulos del Node Editor

	Icono estándar para un módulo de procesado. Su función principal es construir bloques de modelo de nodo.
	Icono estándar usado para un módulo de cola. Lo que le hace diferente del resto de módulos es que el módulo de colas tiene recursos adicionales internos llamados sub-colas.
	Icono usado para un módulo de recibir. Receptor Punto a Punto.
	Icono usado para un módulo de transmitir. Transmisor Punto a Punto.
	Icono usado para un módulo de recibir. Receptor tipo bus.
	Icono usado para un módulo de transmitir. Transmisor tipo bus.
	Icono usado para un módulo de recibir. Receptor por radiofrecuencia.
	Icono usado para un módulo de transmitir. Transmisor de radiofrecuencia.
	Icono estándar usado para las comunicaciones vía satélite.
	Icono estándar para un módulo esys.

FUENTE [10]

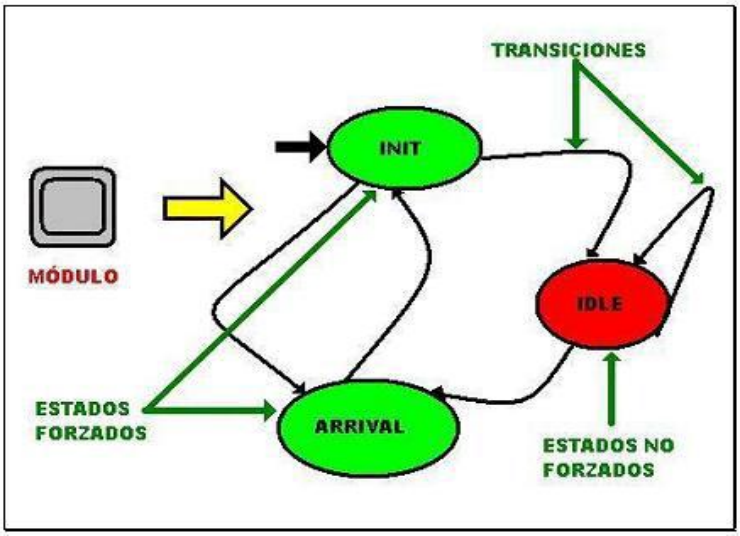
Tabla 2. Conexiones del Node Editor

	*Packet Stream*: Son conexiones que llevan los paquetes desde un módulo fuente a un módulo destino.
	*Statistic wires*: Transportan datos de un módulo fuente a un módulo destino. Sirven como interface para que un módulo fuente pueda compartir datos con un módulo destino, y proporcionar información respecto de su estado.
	*Logical associations*: Su misión es indicar qué relación existe entre dos módulos de la simulación. Por tanto, no trasportan datos entre módulos.

FUENTE [10]

Además se dispone de un modelo de procesos donde se define lo realizado en cada uno de los módulos de un nodo. La figura 15 muestra el funcionamiento explicado anteriormente.

Figura 15. Funcionamiento del módulo de nodos



FUENTE [10]

La funcionalidad de cada módulo se define a través de modelos de proceso, que se representan mediante máquinas de estados finitos (*FSM*). Las transiciones entre estados pueden ser condicionales o incondicionales. El funcionamiento interno tanto de estados como de transiciones implica la programación de código *C/C++.*

Para crear estos modelos de procesos, el software ofrece un editor llamado *process editor*. En éste se pueden definir los estados y las transiciones de los estados. Además, en él se programa el grueso de la simulación en lenguaje *C++*. Una vez se ha creado el modelo de proceso, el siguiente paso es la compilación y la verificación. Para este paso se debe instalar en el computador un compilador de *C++.*[10]

7.3 Partes de OPNET *Modeler*

A continuación se explican las diferentes partes de que consta el OPNET *Modeler*. Los editores incluidos proporcionan las herramientas necesarias para la creación de topologías de red. Cada editor se encarga de una tarea distinta.

7.3.1 *Project Editor:*

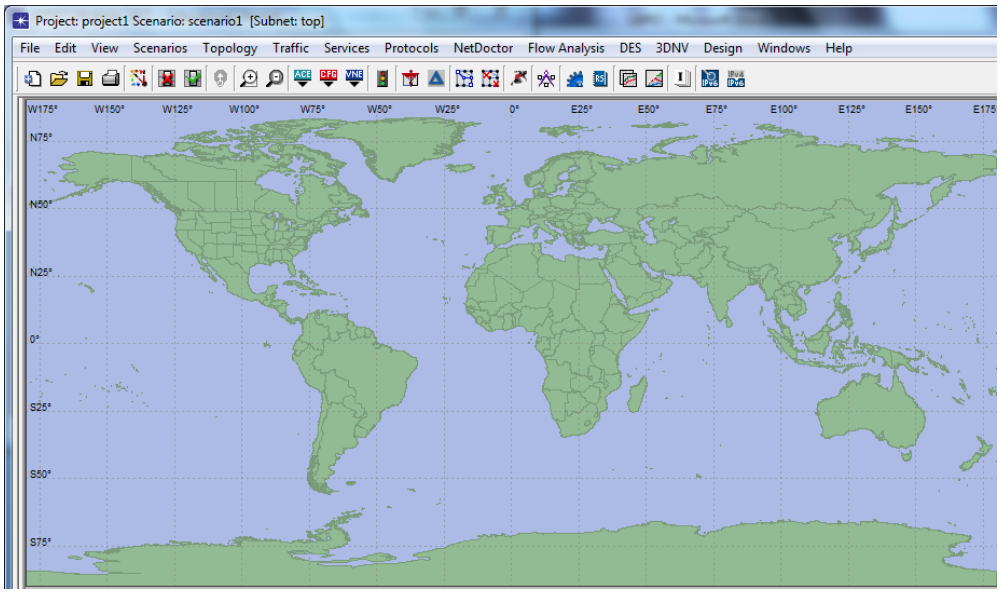
El *Project editor* es el principal escenario en la creación del entorno de la simulación de la red. Es usado para crear un modelo de red utilizando otros ya existentes que se pueden encontrar en la librería estándar, recolectar estadísticas sobre la red, comenzar la simulación y observar los resultados. 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 16), 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 21, 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.[10]

Figura 16. Formato Project Editor



FUENTE [10]

7.3.2 *Node Editor*

El *node editor* es un editor que es usado para crear modelos de nodos especificando su estructura interna. Estos modelos son usados para crear nodos en el interior de la red en el *Project Editor*.

Internamente, los modelos de nodos tienen una estructura modular, al ser definido un nodo como la conexión entre varios módulos con paquetes de *streams* y cables. Esta conexión permite intercambiar información y paquetes entre ellos. Cada módulo tiene una función específica dentro del nodo, tal como: generar paquetes, encolarlos, procesarlos o transmitirlos y recibirlos.

En este editor, los elementos se encuentran disponibles como cajas negras, albergando atributos que pueden ser configurados. Cada una de ellas representa una función en el nodo.
Los objetos presentes en este editor son los procesadores. El comportamiento de éstos viene definido en el editor de procesos. Existen modelos ya configurados, tales como fuentes de datos, sumideros, etc. [10]

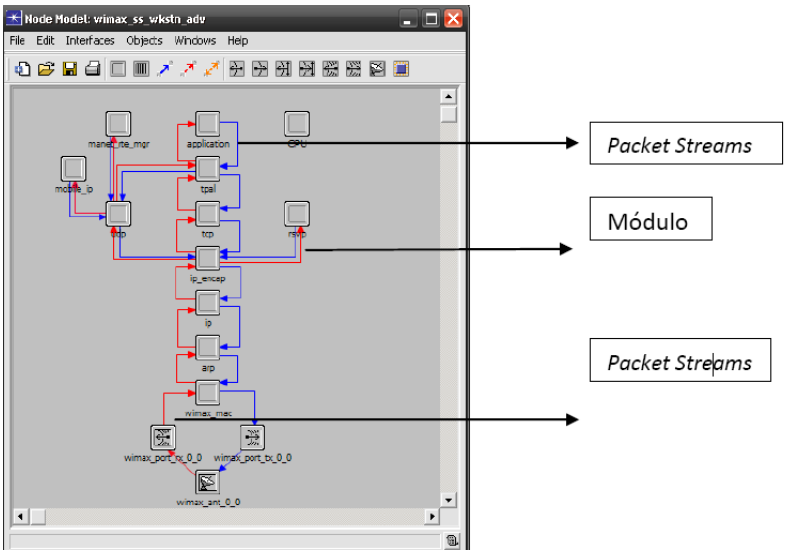
Los procesadores más comunes son:

- **Colas**: Poseen distintos atributos para definir el carácter de la misma.
- **Transmisores y receptores**: Controlan la salida y entrada de paquetes al nodo.
- ***Stream* de paquetes**: Lleva el flujo de paquetes entre cajas negras.
- ***Statistics Wire***: Transporta estadísticas.

Cable de asociación lógica transmisor-receptor: Usado para crear un vínculo entre transmisores y receptores de un mismo elemento.

La estructura de formación de un modelo de nodo se puede visualizar en la figura 17, en ella se muestra tanto el editor de nodos como un pequeño ejemplo en él. En ese ejemplo se logra distinguir los diferentes procesadores que anteriormente se han expuesto.[10]

Figura 17. Node Editor

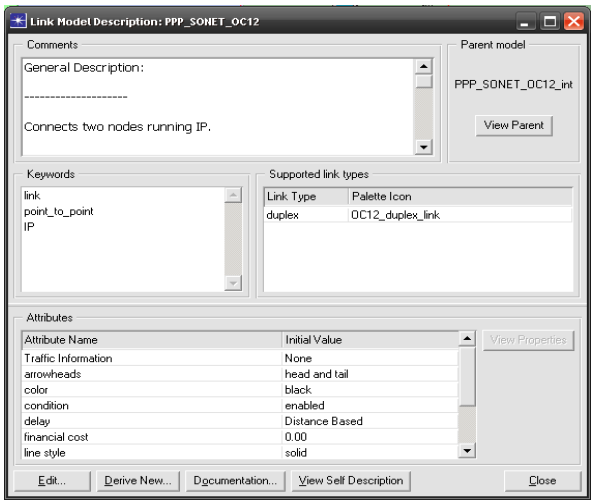


FUENTE [10]

7.3.3 Link Model Editor

Este editor ofrece la posibilidad de crear nuevos tipos de objetos link. Cada nuevo tipo de link puede tener diferentes atributos y representaciones. En la siguiente figura se muestra el editor.

Figura 18.Link Model Editor



FUENTE [10]

Un link model especifica la siguiente información:

- **Tipo de enlace soportado**: Todos los enlaces que soporta el simulador. Estos enlaces son los siguientes: punto a punto duplex, punto a punto simple, bus y taps links.
- **Keyword**: Sirve para simplificar la paleta del project editor y así facilitar el trabajo al programador.

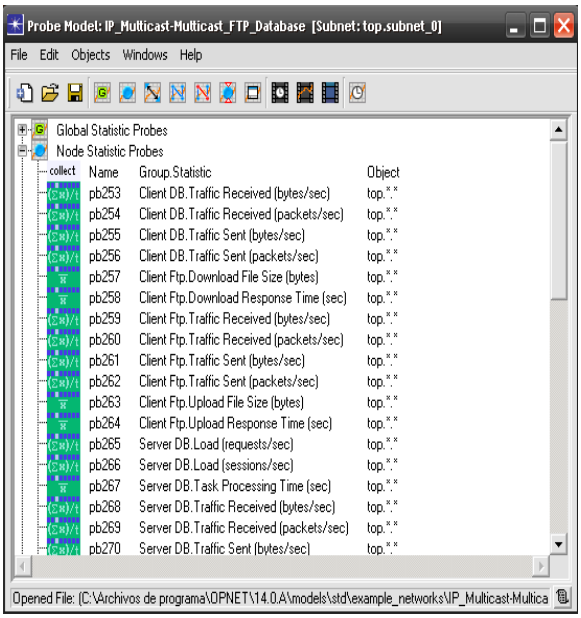
- **Comentarios**: Este apartado permite añadir comentarios a los enlaces. Es muy útil a la hora de utilizar la versión de evaluación ya que no se puede acceder al editor y poder ver lo que hace. Aquí se pueden comentar la capacidad del enlace, las características, etc.

- **Especificación de atributos**: Aquí se pueden cambiar los valores de los atributos puestos por defecto.

7.3.4 Probe Editor

Probe editor es usado para especificar las estadísticas que van a ser recopiladas. Pueden ser de diferentes tipos como: estadísticas globales, de enlaces, de nodos, de atributos, etc. Este editor tiene una representación que podemos contemplar en la siguiente figura.[10]

Figura 19. Probe Editor

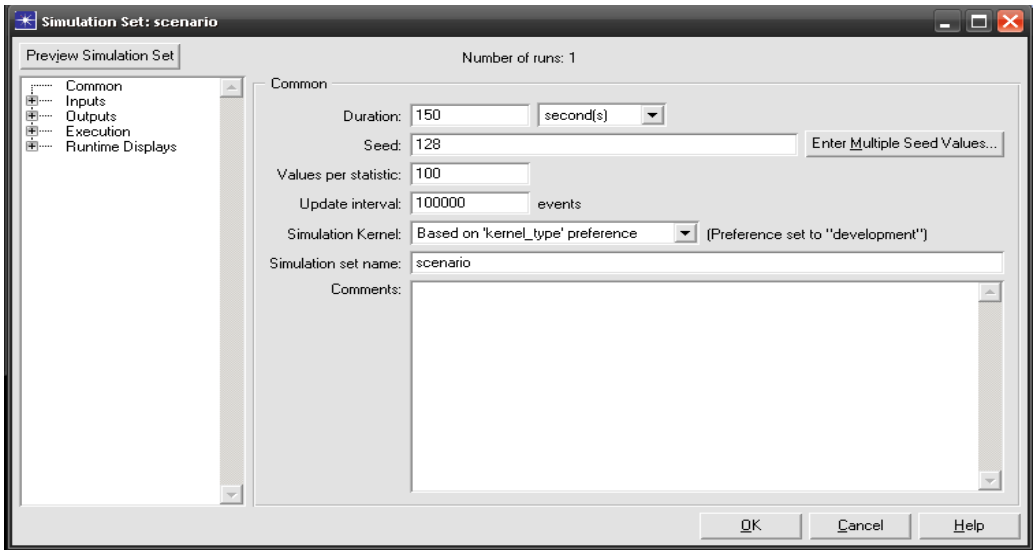


FUENTE [10]

7.3.5 Simulation Sequence Editor

En este editor se pueden añadir valores adicionales específicos tales como el control del tiempo de simulación, la velocidad, etc. En la siguiente figura se puede observar.

Figura 20. Simulation Editor



FUENTE [10]

7.3.6 Analysis Tool

El analysis tool se emplea para crear gráficos escalares de parámetros a estudiar, definir estadísticas de datos, y contemplar los resultados de la simulación. En la siguiente figura se puede detallar este editor.[10]

Figura 21. Analysis Tool

FUENTE [10]

7.3.7 Simulación *DES*

Se ha comentado anteriormente que el entorno de simulación OPNET utiliza la tecnología *DES* (*Discrete event simulation*). Ahora se dispondrá a exponer de qué trata esta tecnología.

En una simulación *DES* se utilizan eventos para describir sucesos o acciones que tienen lugar en un determinado momento. Cada uno de estos eventos tiene un instante de incidencia puntual en la escala temporal. Esta escala, al igual que el resto de magnitudes, es discreta.

Durante la simulación, se puede distinguir entre el tiempo real y el tiempo de simulación, por ello se utilizan variables contador para representar el momento actual y las cantidades de tiempo. También se utilizan varias variables de estado para representar la fase del sistema simulado. Por lo que se refiere al sistema, evoluciona en la memoria del computador, produciéndose diferentes eventos que edifican las variables de estado, y éstas a su vez determinan los futuros eventos.

Cada evento tiene un instante de incidencia puntual, es decir, pueden ser representados sobre la escala temporal discreta de la simulación ocupando una única posición. De este modo, dichos eventos logran ser ordenados cronológicamente, según su instante de incidencia, para ser procesados. En este tipo de simulación, el evento es la unidad de ejecución. Cada uno describe una acción, y el resultado de ésta es la modificación de las variables de estado. Esta característica está especialmente soportada por los lenguajes *OOP* (programación orientada a objetos).

Así pues, un simulador *DES* debe tener un bloque que inicialice todas las variables de estado del sistema simulado, un procesador que ejecute eventos, un planificador (*scheduler*) que sincronice los bloques asegurando que los eventos se ejecutan en el orden adecuado y un recolector de datos estadísticos que tome nota de lo ocurrido. Por último, al finalizar la simulación o de manera dinámica durante su ejecución, se podrán procesar los datos recogidos para extraer la información deseada con la posibilidad de representarlos de forma gráfica.

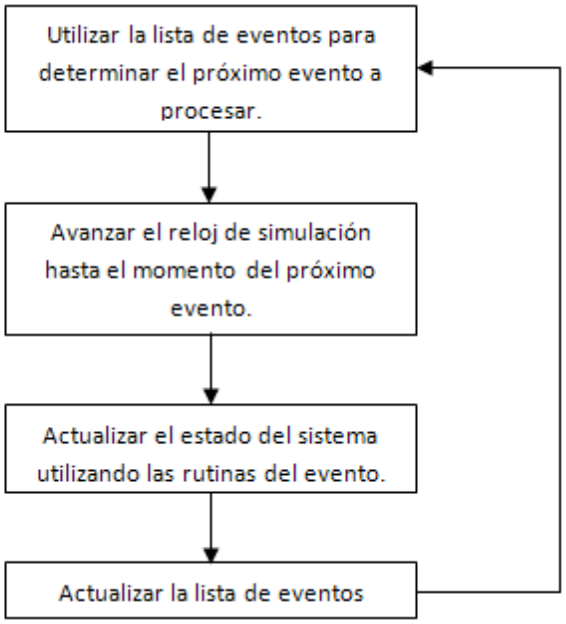
Entretanto, la simulación se repite de forma continuada en un diagrama de bloques que en cada iteración recoge el primer evento a procesar. A continuación se ejecuta éste y modifican sus variables de estado, después avanza el contador de tiempo hasta el momento de incidencia del próximo evento, y se reinicia el bucle.

Como se ha mencionado anteriormente, el contador de tiempo no avanza de manera constante, sino que salta directamente el tiempo restante desde el primer instante actual hasta la incidencia del próximo evento, siendo este periodo aleatorio y determinado por la secuencia de eventos.

Durante la actualización del contador de tiempo y la modificación de las variables de estado, pueden generarse nuevos eventos que se insertarán en la lista de

eventos a procesar o modificarán los atributos de los ya existentes. El proceso mencionado se detalla en la figura 22.[12]

Figura 22.Proceso Simulación



FUENTE [10]

[12] OPNET: Manual de usuario. Departamento de Ingeniería Telemática. Universidad Politécnica de Cataluña. 2004.

8. DESARROLLO DE LA TESIS

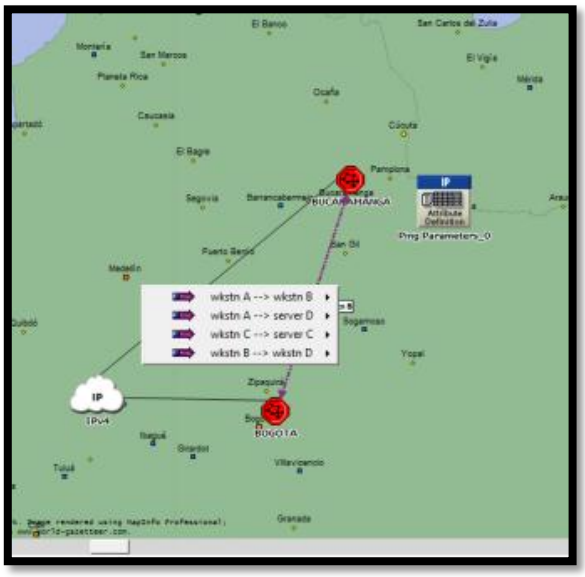
8.1 PRUEBAS REALIZADAS

8.1.1 PRUEBA 1: TUNNEL MANUAL y TUNNEL IPSec

8.1.1.1 Descripción del escenario

En esta prueba se realizo un escenario que se compone de 2 redes que están conectadas mediante una nube IPv4. Contiene dos routers dentro de las Subnets que hacen la interconexión entre Bogotá y Bucaramanga; ya que los enrutadores no se encuentran directamente conectados porque se enlazan a una red trocal (IPv4). Además contiene temas como: RIP, RIPNG y configuración de la aplicación PING.

Figura 23.Escenario Tunnel Manual



Autores

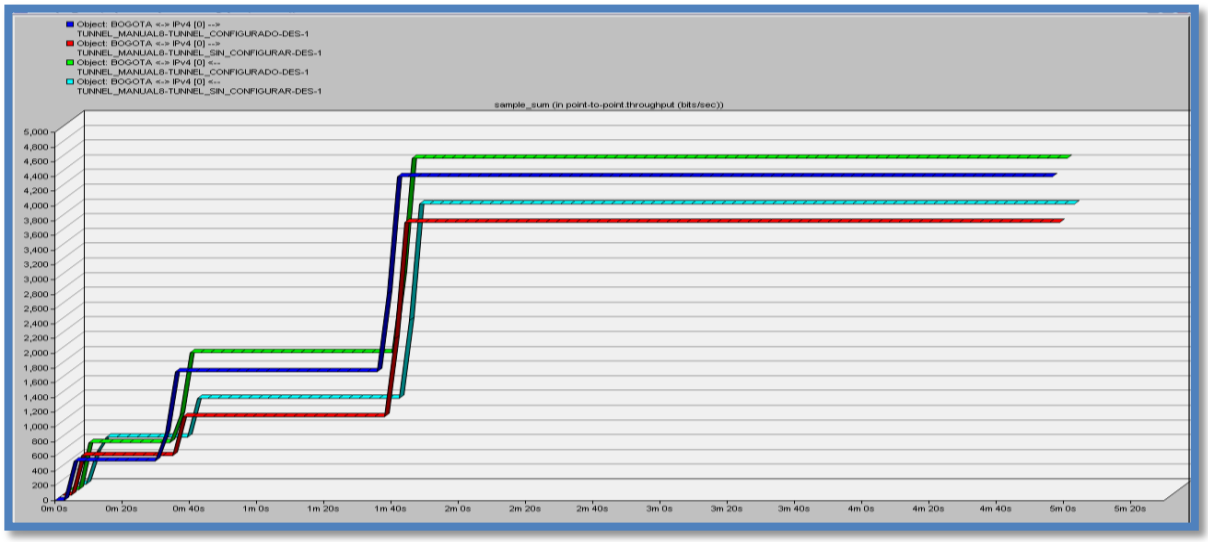
8.1.1.2 Resultados

BOGOTÁ – IPv4

Escenario Tunnel Manual configurado y Manual sin configurar

Throughput (bits /sec)→, Throughput (bits /sec)←

Figura 24.Resultados del rendimiento en los Escenarios en (bits/sec) en el enlace Bogotà-IPv4



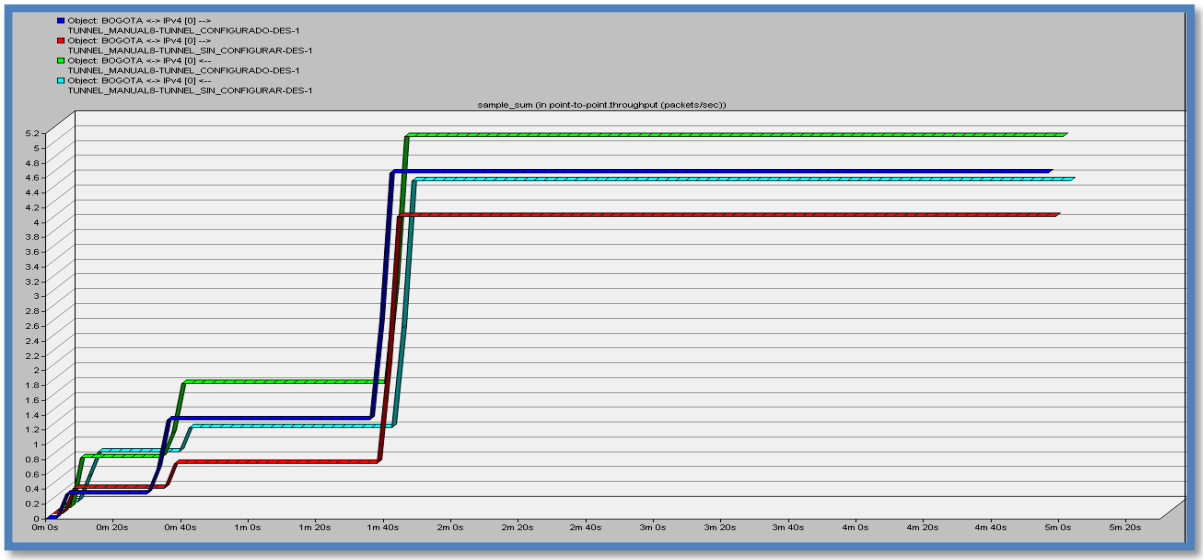
Autores

BOGOTÁ – IPv4

Escenario Tunnel Manual configurado y Manual sin configurar

Throughput (packets /sec)→, Throughput (packets /sec)←

Figura 25.Resultados del rendimiento en los escenarios en (packets/sec) en el enlace Bogotà-IPv4



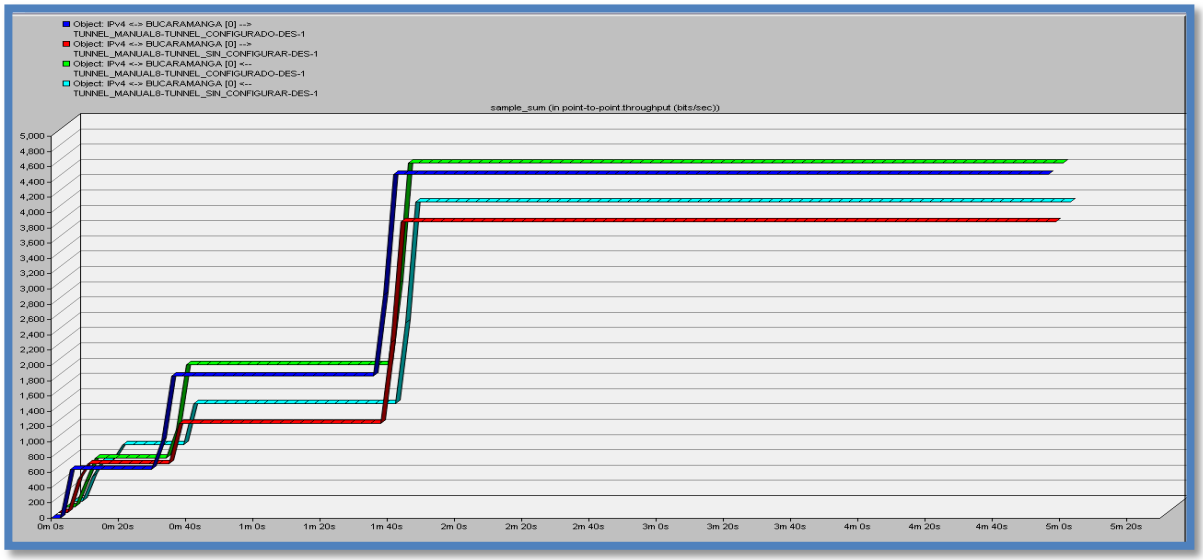
Autores

IPv4- BUCARAMANGA

Escenario Tunnel Manual configurado y Manual sin configurar

Throughput (bits /sec)→, Throughput (bits /sec)←

Figura 26.Resultados del rendimiento en los escenarios en (bits/sec) en el enlace IPv4-Bucaramanga



Autores

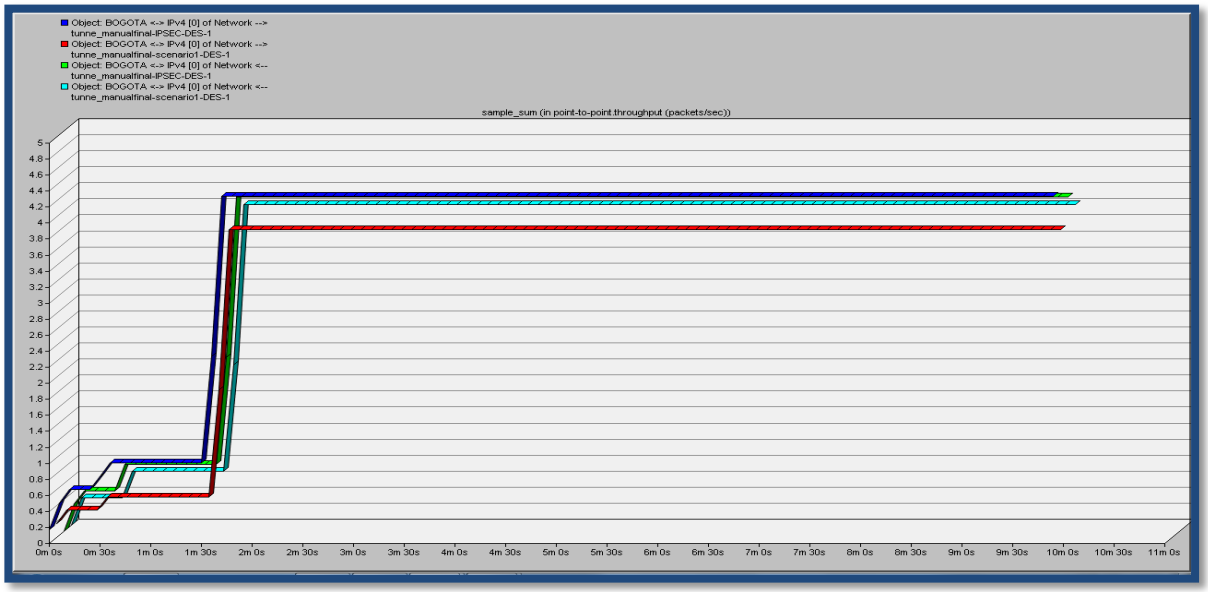
COMPARACION DE TUNNEL MANUAL Y TUNNEL IPSec

BOGOTÁ – IPv4

Escenario Tunnel Manual configurado y Tunnel IPSec

Throughput (bits /sec)→, Throughput (bits /sec)←

Figura 27.Resultados del rendimiento en los escenarios en (packets /sec) en el enlace BOGOTÀ-IPv4



Autores

8.1.1.3 Análisis de resultados

En las gráficas anteriores de los escenarios Tunnel Manual configurado y Tunnel Manual sin configurar en (bits/sec) y (packets/sec) de los enlaces entre Bogota-IPv4 e IPv4-Bucaramanga, del trafico recibido y enviado, se logra observar que efectivamente al configurar el Tunnel Manual, el ancho de banda aumenta debido, a que los paquetes de IPv6 se encapsulan dentro de los paquetes IPv4, permitiéndole viajar por la red hasta llegar a su destino final.

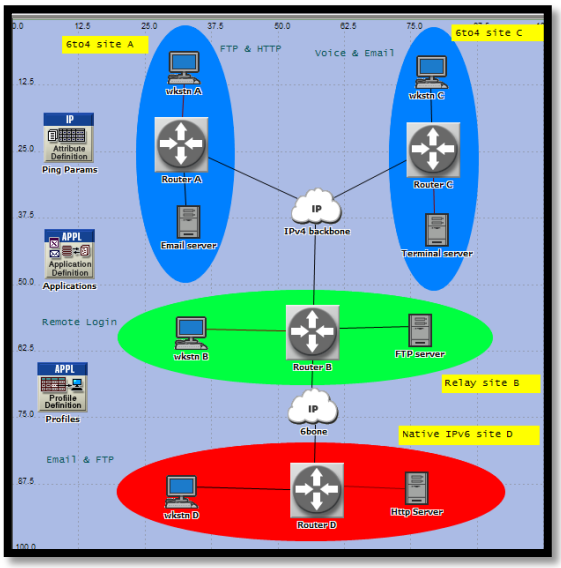
En la graficas que muestra la comparación de tunnel manual y tunnel IPSec se logra visualizar el tráfico enviado y recibido y como varia en ancho de banda de un túnel a otro.

8.1.2 PRUEBA 2: TRANSICIÒN DE IPV6 A IPV4 DE FORMA AUTOMÀTICA.

8.1.2.1 Descripción del escenario

El escenario realizado consta de dos sitios (sitio A y B) 6to4 que se encuentran conectados a través de una red troncal IPv4, por medio de tuneles 6to4 donde la configuración se realiza en los routers A y C. Para lograr comunicarse con otros destinos (sitio B). Tanto los routers A y C tienen una ruta predeterminada al enrutador B, los paquetes que serán enviados desde el sitio A al sitio nativo D, primero tendrán que ser encapsulados y enviados al router B, por medio de tuneles 6to4, que tiene como función encapsular y desencapsular para poder ser entregados al sitio final. Con la construcción de esta práctica, se permite enviar paquetes IPv6 sobre redes IPv4, sin la necesidad de configurar tuneles manualmente.

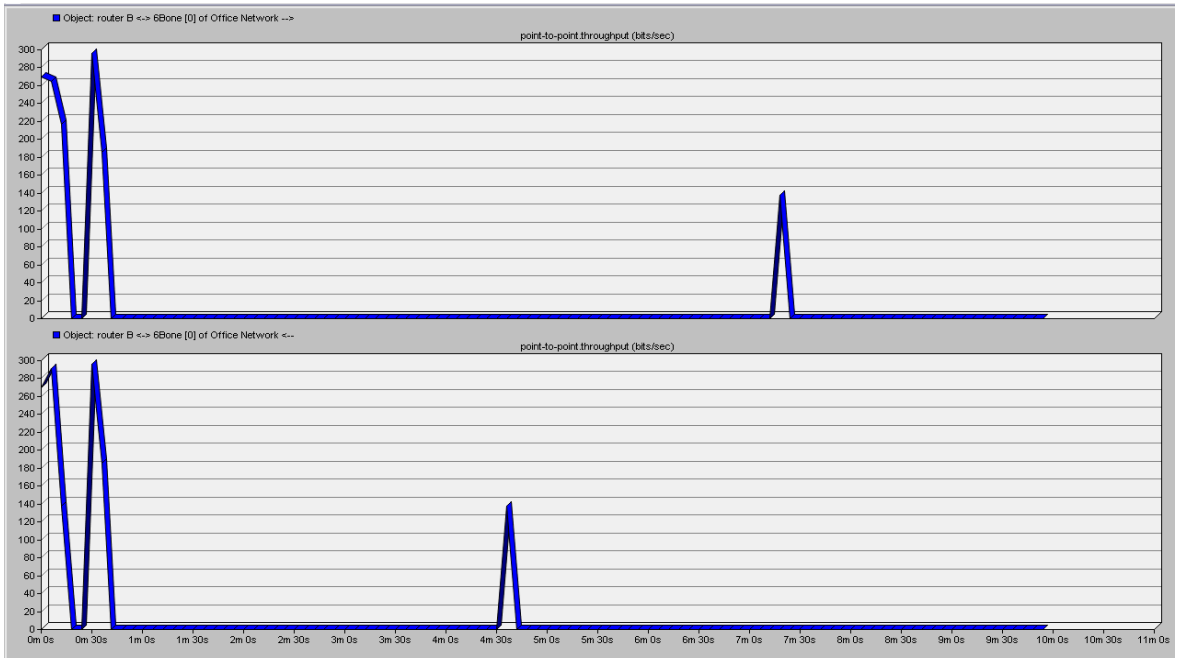
Figura 28.Escenario 6TO4



Autores

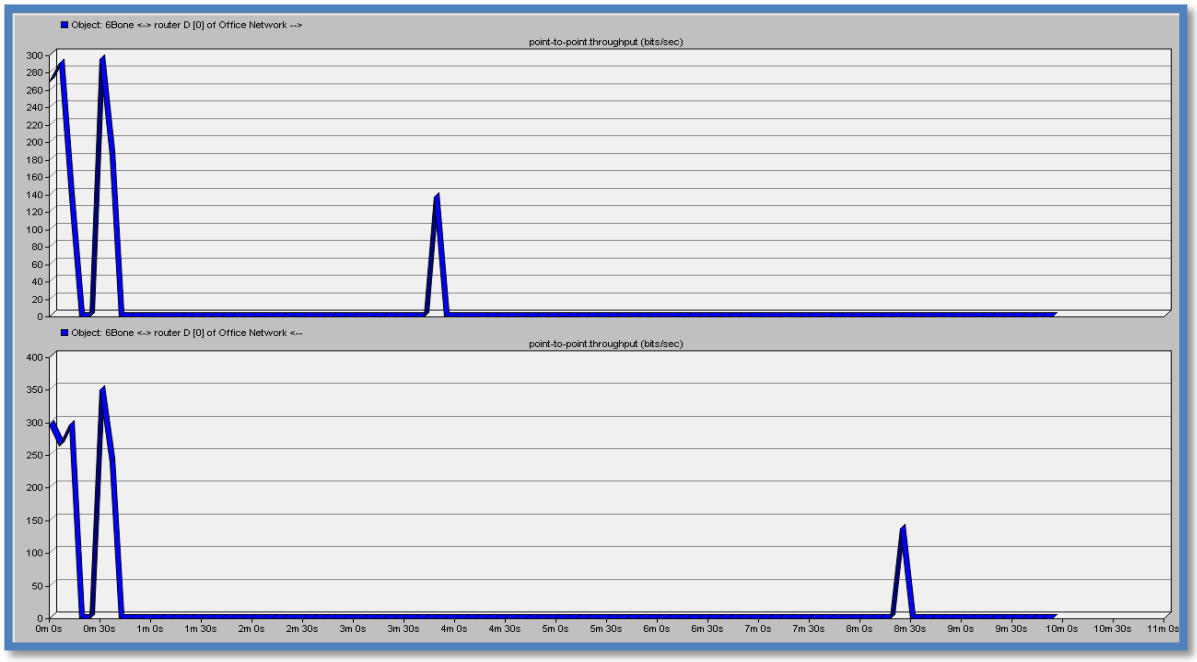
8.1.2.2 Resultados

Figura 29.Resultados del tráfico de Router B- 6bone



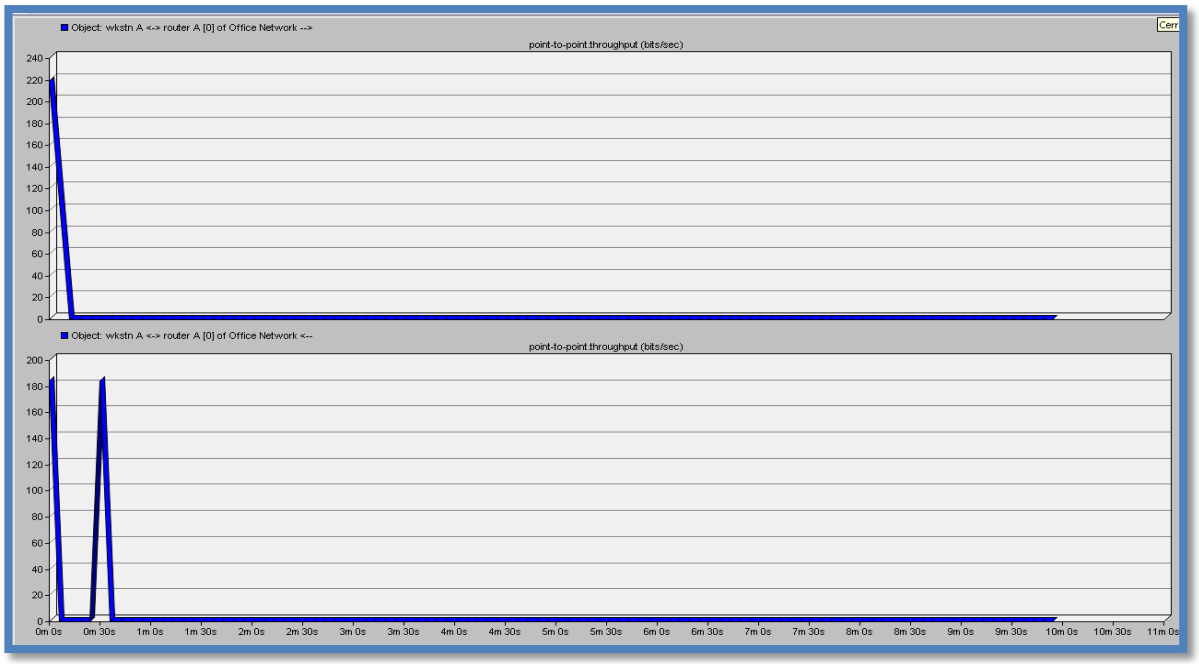
Autores

Figura 30.Resultados del tráfico de 6bone – Router D



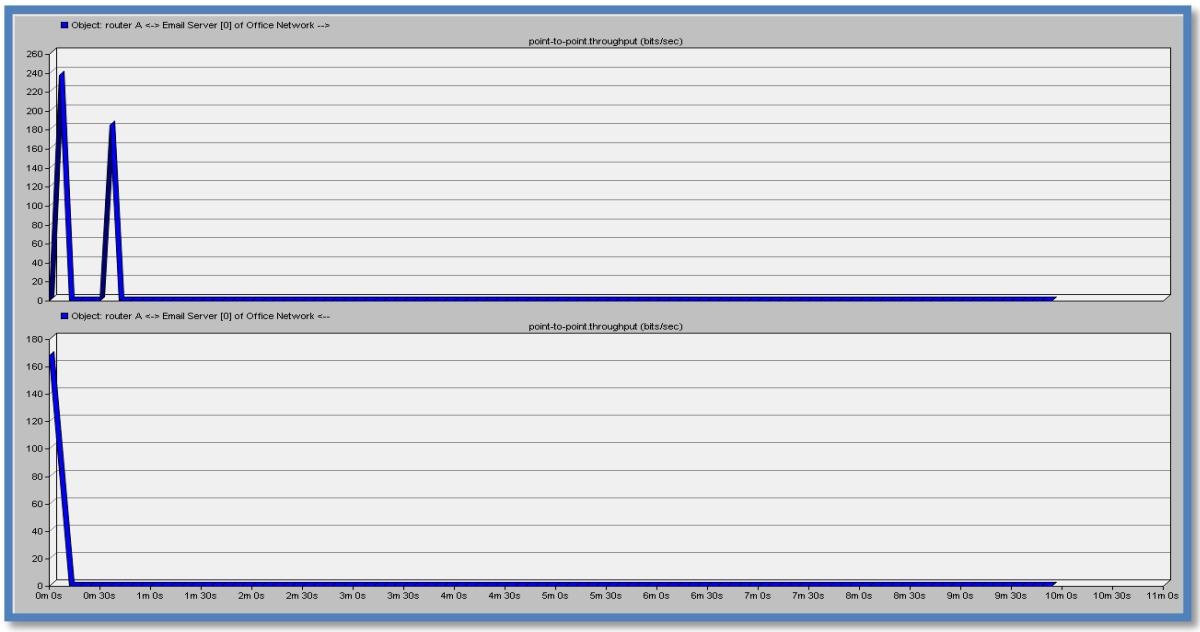
Autores

Figura 31.Resultados del tráfico de Wkstn A- Router A



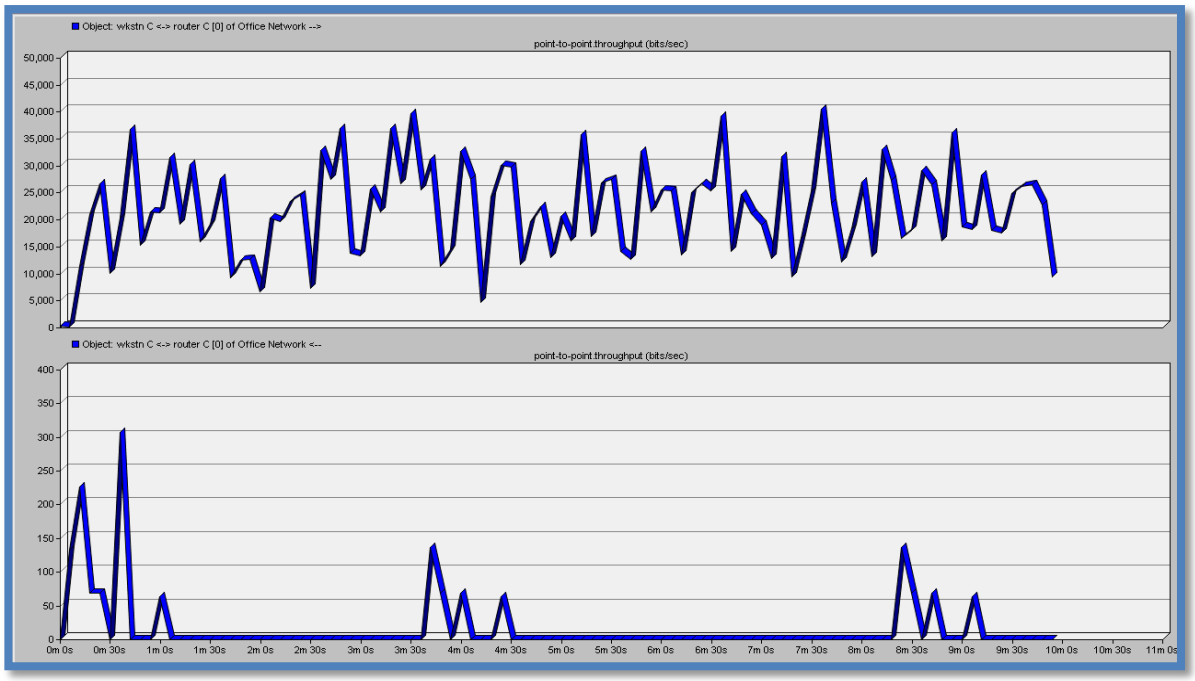
Autores

Figura 32.Resultados del tráfico de Router A – Email Server



Autores

Figura 33.Resultados del tráfico de Wkstn C - Router C



Autores

8.1.2.3 Análisis de resultados:

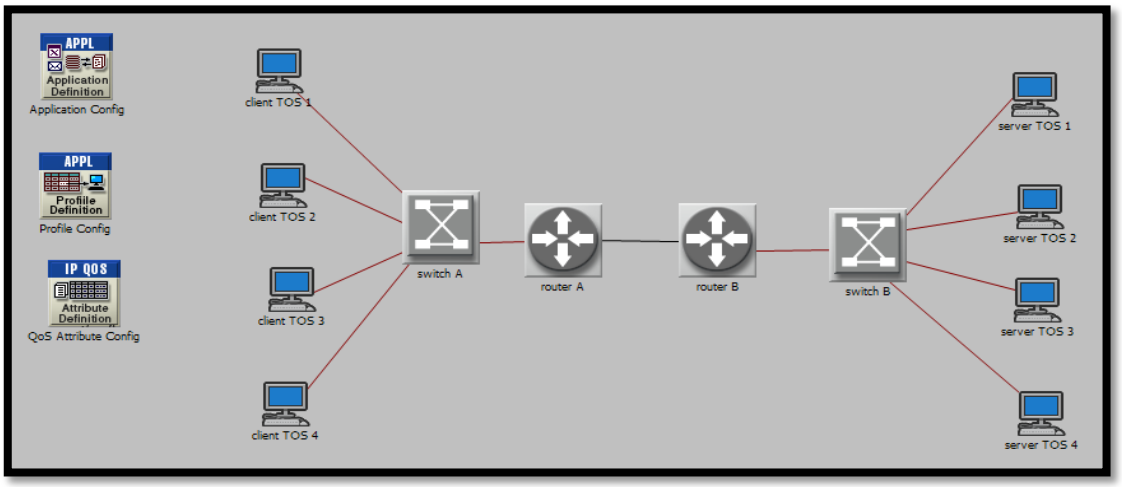
En las gráficas anteriores se observó que efectivamente se está enviando y recibiendo tráfico entre la estación y el router, y entre el router y el servicio, además se observa que se encuentra configurado el mecanismo de transición 6to4 que permite que se puedan enviar paquetes IPv6 sobre redes IPv4 atravesando la red. Todos los routers en la red nativa de IPv6 tienen una ruta estática al destino (cuya dirección IPv6 es 2002::/16) en la cual el siguiente salto será el router B. Entonces si cualquiera de estos router recibió un paquete destinado para un nodo en los sitios A o C, este será transmitido al router B, quien será capaz de tunelizar el paquete de forma correcta. Para finalizar el 6to4 es un mecanismo de transición que permite que IPv6 sea encapsulado en paquetes Ipv4, de forma que puede pasar solo redes IPv4, y también permite el tránsito de IPv6 a través de un proveedor de servicios de internet, que solo ofrecen servicio IPv4.

8.1.3 PRUEBA 3: CALIDAD DE SEVICIO CON UN ALGORITMO DE PLANIFICACIÒN.

8.1.3.1 Descripción del escenario

La red está compuesta de clientes y servidores, cada par usa un ToS diferente para la transferencia de datos. El switch A y B, tienen la función de capa de acceso. Los client ToS 1 y 3 generan tráfico IPv4 y los client 2 y 4 generan tráfico IPv6. Los sistemas finales (cliente-servidor) poseen diferentes aplicaciones como; Email, File Transfer, Video Conferencing, etc. El algoritmo de planificación que se utiliza para que los enrutadores ofrezcan calidad de servicio es el MDRR, ya que se presenta una situación en cuello de botella. Las clases de tráfico que se utilizan en esta práctica son para clasificar los paquetes según su prioridad y brindar soporte de QoS, según las políticas de tráfico.

Figura 34.Escenario Calidad de Servicio



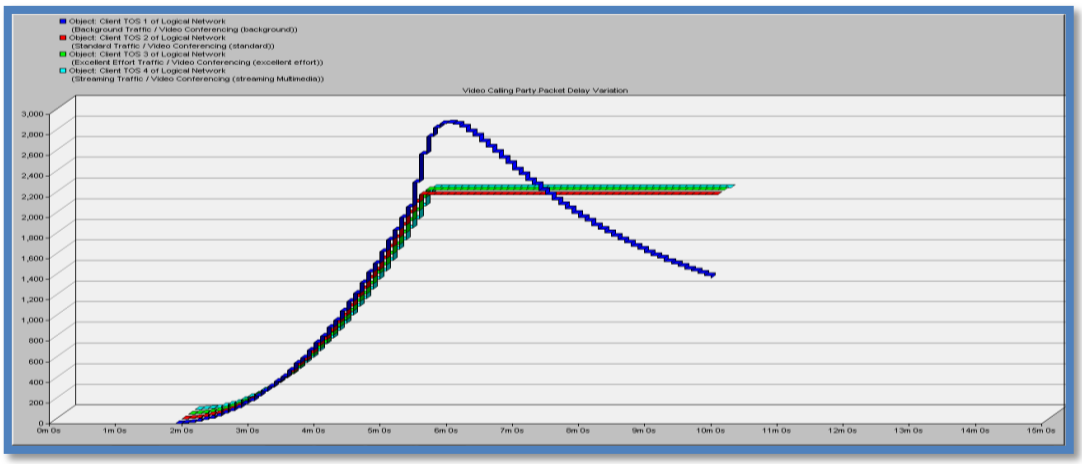
Autores

8.1.3.2 Resultados

Resultados de los client ToS 1, client ToS 2, client ToS 3 Y client ToS 4. Video Called Party.

Video calling Party: Packets Delay Variation

Figura 35.Resultados del tiempo de variación de los paquetes en cada client

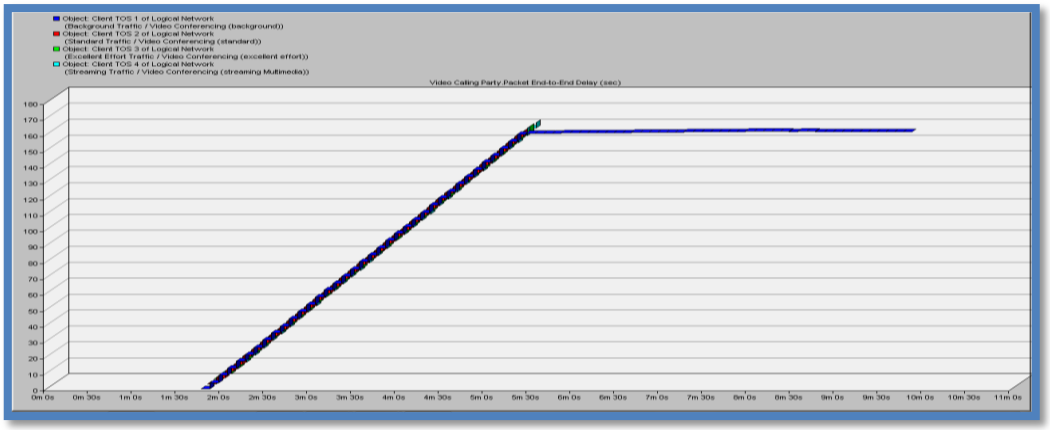


Autores

Packect End-to-End Delay

Muestra el tiempo que transcurre cuando un paquete es enviado por una aplicación (video) y recibido en un servidor que lo soporte.

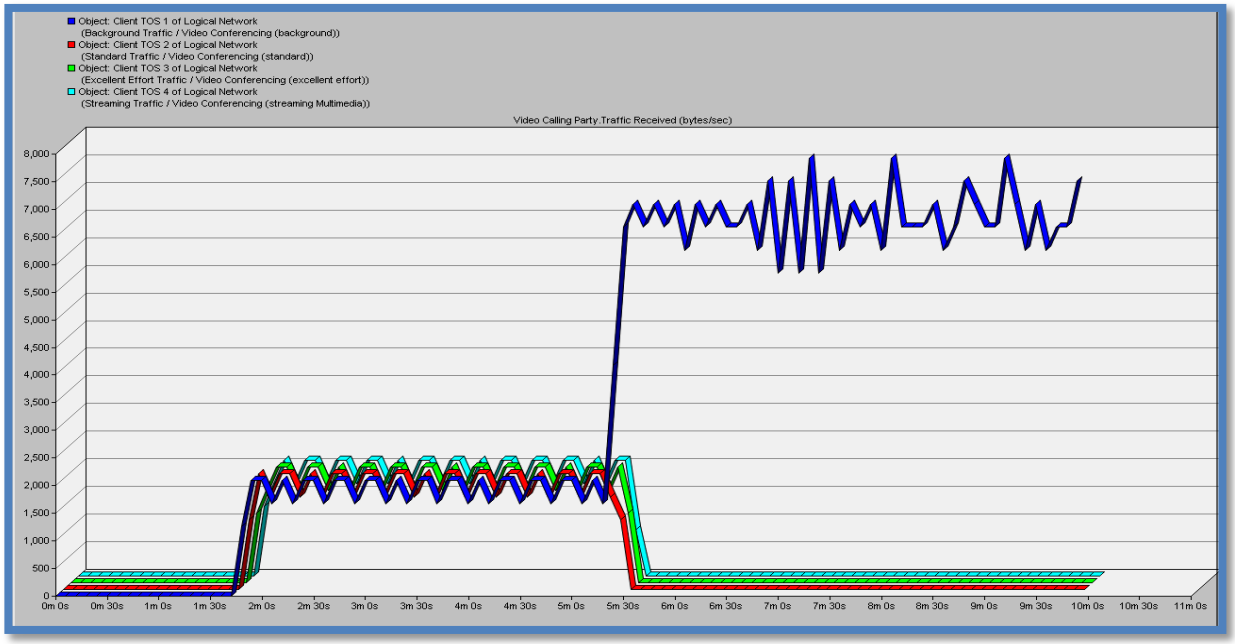
Figura 36.Resultados los paquetes End-to End



Autores

Traffic Received (bytes/sec)

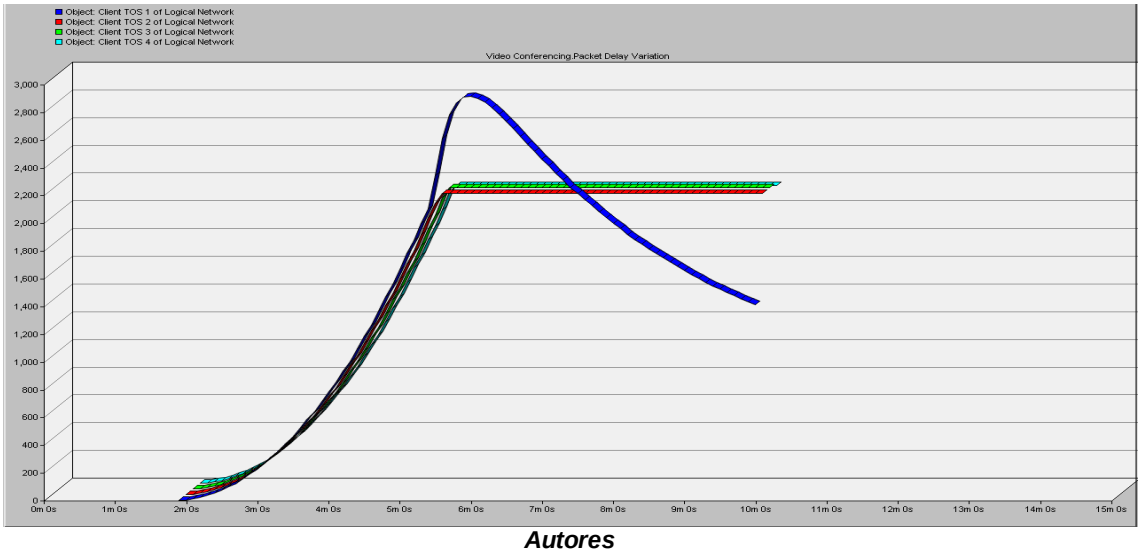
Figura 37.Resultados Tráfico recibido en (bytes/sec)



Autores

Video Conferencing: Packet delay Variation analiza la variación de la transmisión y recepción de paquetes que hay en cada client.

Figura 38.Resultados de la variación de paquetes de Video Conferencing

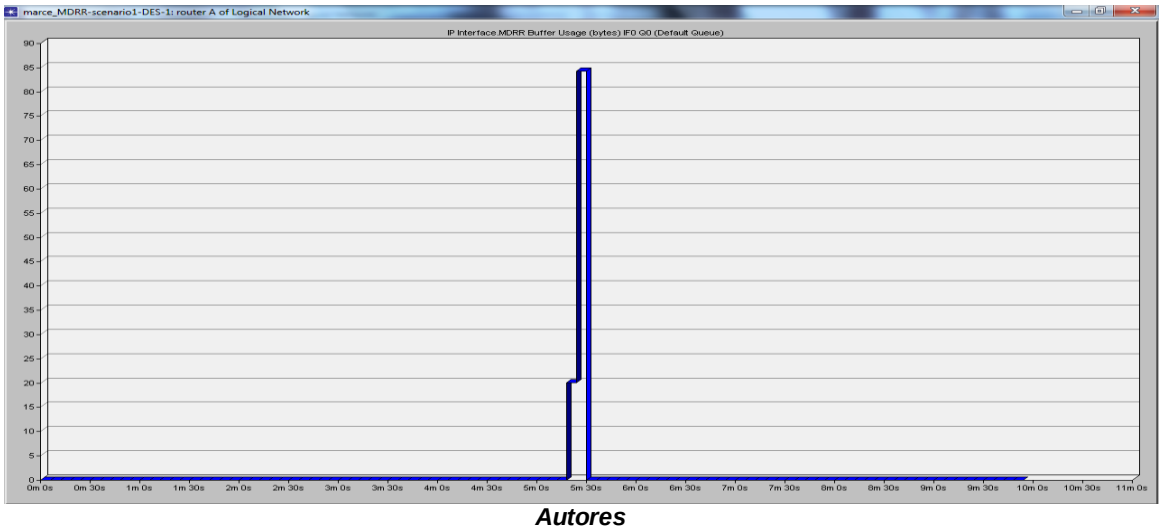


Autores

Gráficos del router A.

IP Interface. MDRR Buffer Usage (bytes) IF0 Q0 (Default Queue)

Figura 39.Resultados del buffer

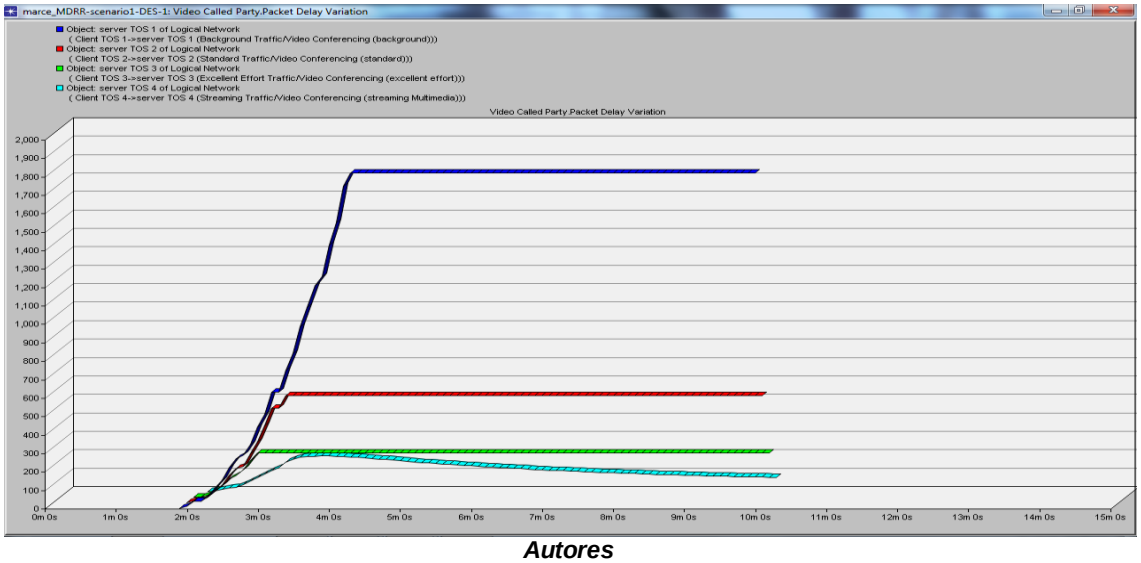


Autores

Resultados de los server ToS 1, server ToS 2, server ToS 3 Y server ToS4.

Video Called Party. Packet Delay Variation

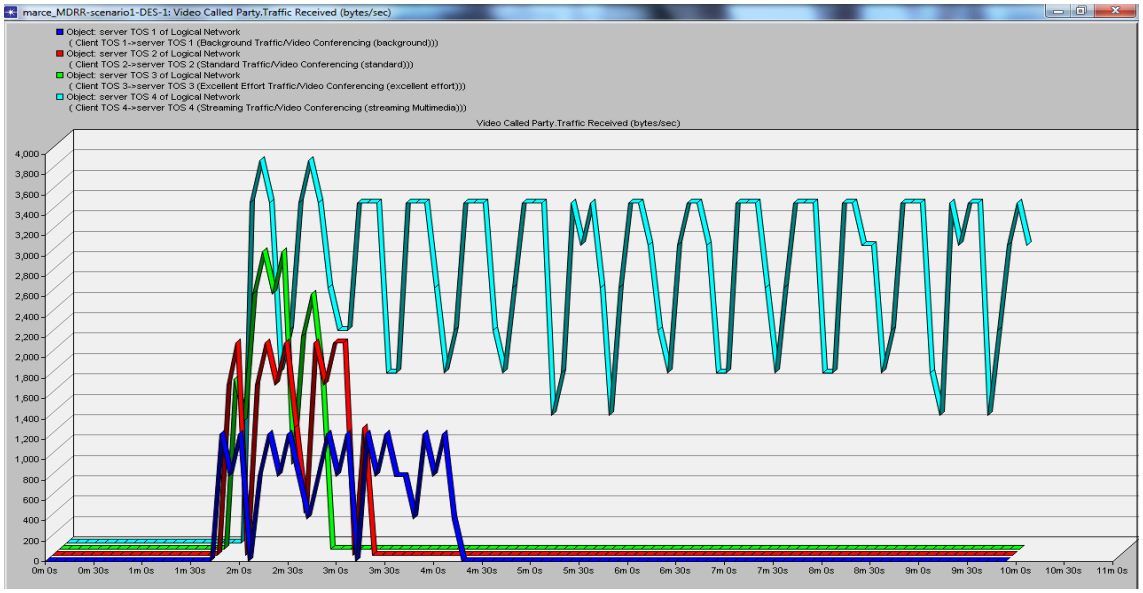
Figura 40.Resultados del tiempo de variación de los paquetes en cada server



Autores

Traffic Received (bytes/sec)

Figura 41.Resultados del tráfico recibido en cada server



Autores

8.1.3.2 Analisis de Resultados

- ✓ Se logra observar el tiempo de retardo de los paquetes recibidos por el nodo de video calling party de cada servidor; medido desde que es enviado hasta el momento de recepción.

- ✓ Se observa el tráfico recibido en cada servidor, el cual muestra al diferencia entre cada aplicación; envía mayor tráfico el server que soporta la aplicación en background ya que tiene la mayor prioridad en el escenario.

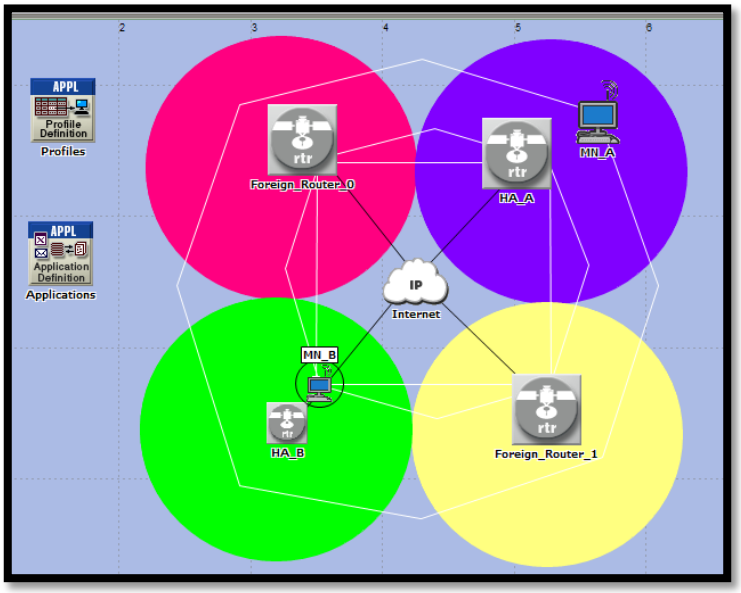
- ✓ IP Interface. MDRR Buffer Usage (bytes) IF0 Q0 (Default Queue); Este parámetro mide el tamaño de la cola de espera de trasmisión dado que cada aplicación tiene una prioridad diferente por tanto un client puede enviar paquetes más rápidos, mientras otros más lentos. En la gràfica el punto más alto muestra el valor en bytes de la información en espera, también se logro aprecià que el tiempo de espera es muy corto.

8.1.4 PRUEBA 4: MOVILIDAD EN IPv6

8.1.4.1 Descripción del escenario

La red MIPV6 tiene cuatro puntos de acceso WLAN conectados a través de una nube IP. EL núcleo de red, representado por la nube IP. MN_A y MN_B se comunican entre sí mediante la aplicación de video muy ligera como una fuente constante de tráfico UDP. Inicialmente los móviles se colocan en sus redes de origen correspondiente (Home Networks). Entonces el MN_A (Mobile Node A) es servido por el agente de local HA_A (home agent A) y la estación MN_B (Mobile Node B) es servida por el agente de local HA_B (home agent B). Ambos móviles usan MIPV6 para recorrer varios puntos de acceso en la red. El movimiento que realiza el nodo MN_A es una trayectoria anti horaria, y el nodo MN_B, realiza una trayectoria horaria, que les permite recorrer los cuatro puntos de la red.

Figura 42.Escenario Movilidad IPv6

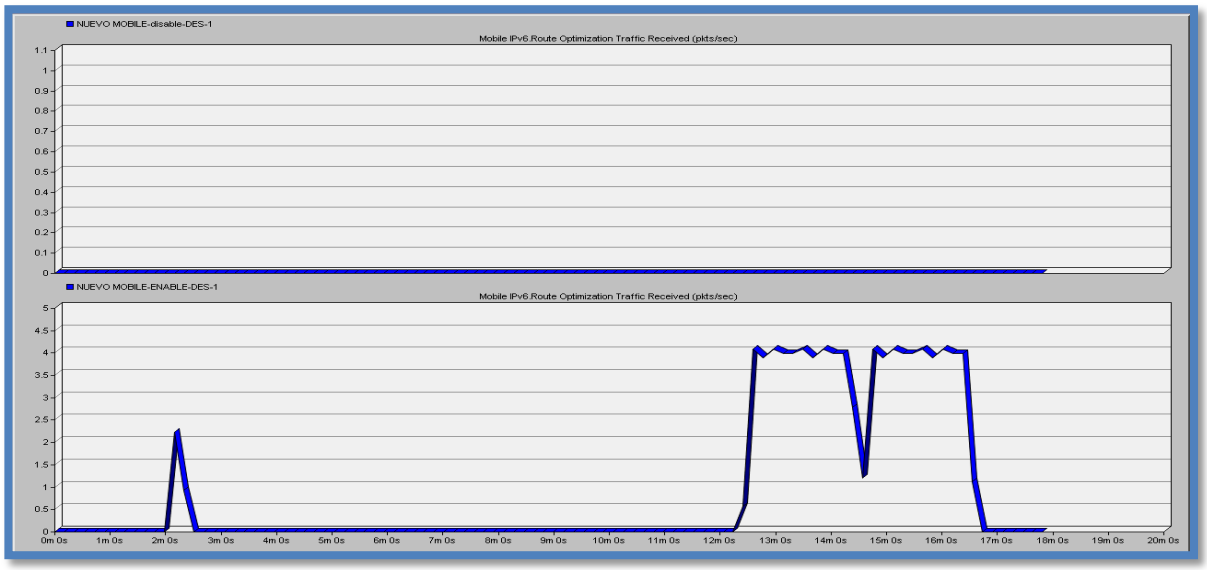


Autores

8.1.4.2 Resultados

Route Optimization Traffic Received (pkts/sec)

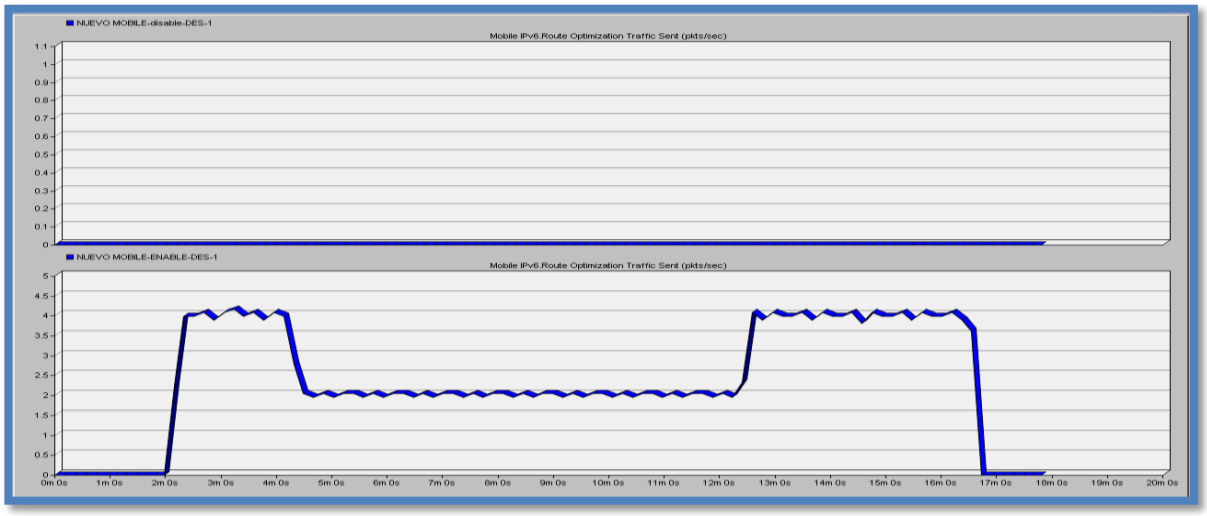
Figura 43.Resultados del tráfico recibido en la ruta optimizada



Autores

Route Optimization Traffic Sent (pkts/sec)

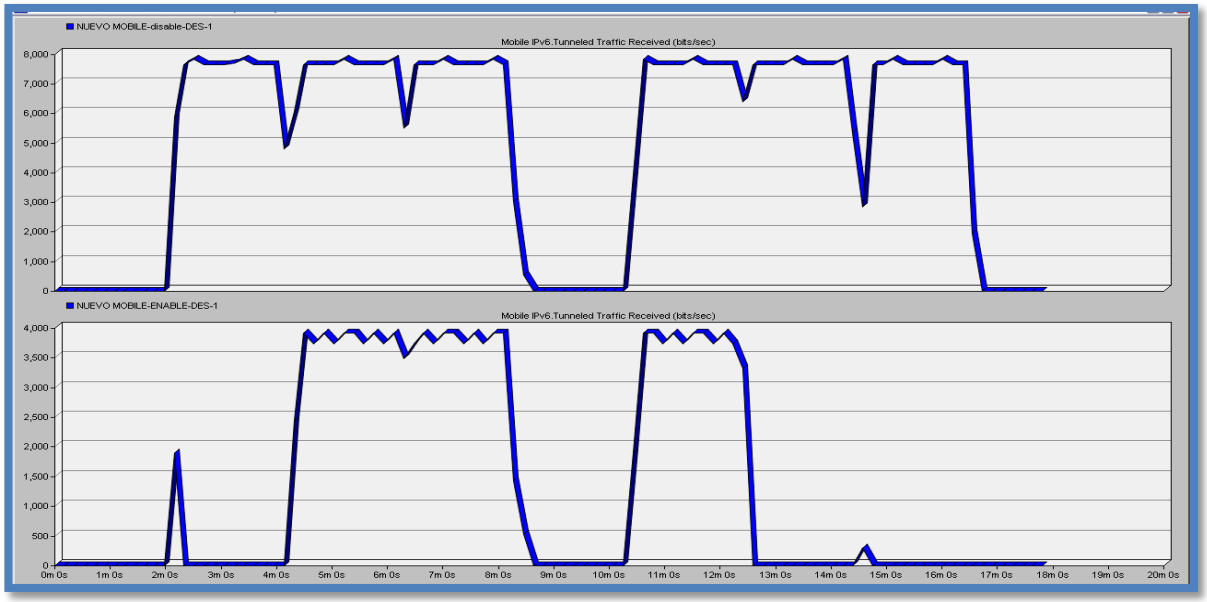
Figura 44.Resultados del tráfico enviado en la ruta optimizada



Autores

Tunneled Traffic Received (bits/sec)

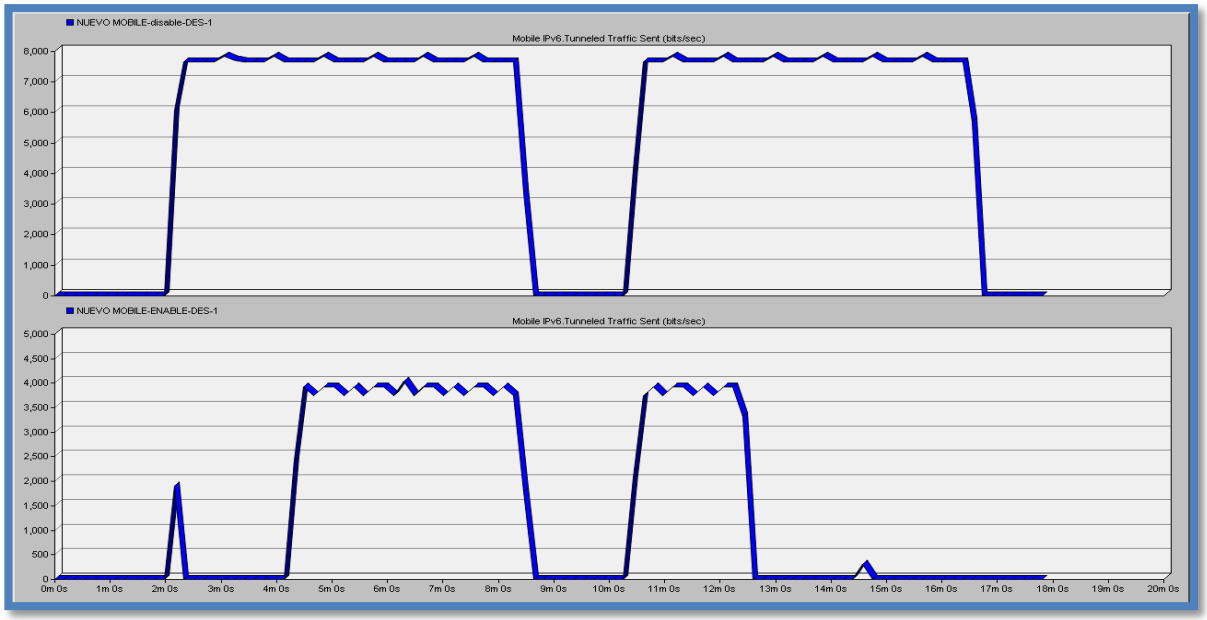
Figura 45.Resultados del tráfico recibido en el tunnel



Autores

Tunneled Traffic sent (bits/sec)

Figura 45.Resultados del tráfico enviado en el tunnel



Autores

8.1.4.3 Análisis de resultados:

- ✓ El problema actual que existe en IPv4 Móvil, consiste en el enrutamiento ineficiente o triangular, ya que el trayecto del triangulo es formado desde el nodo móvil, hacia un nodo correspondiente y el agente local forma el tercer vértice y administra el camino que toman los datos desde el nodo correspondiente hacia el nodo móvil, este tipo de enrutamiento origina un retardo a la hora de entregar paquetes y produce una carga innecesaria sobre las redes y enrutadores. Para corregir este problema se añadieron rutas de optimización a las operaciones que realiza IP móvil, para que los paquetes sean enrutados de tal forma que se impida el paso por el agente local.
- ✓ La movilidad de IP consiste en la capacidad que tiene la máquina para poder mover su conexión de red de un punto de Internet a otro sin cambiar su dirección IP y no perder conectividad. Entonces la movilidad IP soluciona este inconveniente, asignando un IP fija al dispositivo móvil, usando encapsulación IP (Tunneling) con el encaminamiento automático para asegurar que los datagramas destinados a ella se encaminen a la correcta dirección IP que se está usando en ese momento. En las gràficas anteriores se observa que efectivamente se está realizando este proceso, ya que se está recibiendo y enviando tráfico a través de los túneles.

CONCLUSIONES

- Se analizò que el enrutamiento ineficiente o triangular, que tenia MIPV4, y tiene como solución la implementación de MIPv6, ya que este puede encaminar paquetes directamente desde un nodo correspondiente (CN) a cualquier nodo móvil, obviando la necesidad que crucen una red local y en definitiva que sean reenviados por el agente respectivo. Cabe mencionar que MIPv6 envía paquetes a un nodo móvil que esta en una red foránea y llevan una cabecera de encaminamiento entonces requiere menos bytes adicionales de encabezado y con este modo se reduce lo que se llama ‘’overhead del paquete”, los MIPv4 llevan una cabecera de encapsulamiento adicional.

- Se comprendió el envió de paquetes con el mecanismo de transición Tunnel Manual, realizando configuraciones manuales.

- Se analizò e implemento el procedimiento para enviar y recibir paquetes IPv6 a través de túneles IPv4 utilizando servicios como Email Server, Terminal Server, FTP Server y Http Server.

- Se observò el comportamiento de tuneles en redes IPv6 y ademàs se comprobó paràmetros importantes como ancho de banda y rendimiento que podría llegar a tener la implementación de este protocolo.

TRABAJO FUTURO

En este proyecto se realizaron prácticas de laboratorio que explican el funcionamiento y el mejoramiento de IPv4 a IPv6 en sus diferentes temas nombrados anteriormente.

Las recomendaciones a futuro es visualizar otros temas que tengan afinidad con IPv6 y su implementación en el mundo. Ademàs, seguir investigando y acercando a la academia a la realización de este tipo de proyectos para que sean utilizados y aplicados en materias de pregrado y posgrado.

BIBLIOGRAFÌAS

[1] BEHROUZ A FOROUZAN. *Transmisión de Datos y Redes de Comunicaciones.* 2da edición. 2002. *Mc Graw Hill*.

[2] REDES DE COMPUTADORES un enfoque descendente Basado en Internet. 2da edición. 2004. PEARSON Addison Wesley

[3] Características del protocolo de internet 6; [día 19 de junio 2010, hora 2:30pm] página en internet [http://www.rau.edu.uy/ipv6/queesipv6.htm#10]

[4] RFC2373, Arquitectura de Direccionamiento en IPv6

[5] TEORIA Y METODOS DE TRANSICION IPv4 e IPv6 6; [día 10 de mayo 2010, hora 10:30 am] página en internet:

[http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf]

[6] CALIDAD DE SERVICIO MULTICAPA EN UNA RED IP BASADA EN WIMAX, Tesis de pregrado de Julieth katherin Ariza Olarte y Sergio Manuel Racini Bueno

[7] Contribución al soporte de Calidad del Servicio en Redes Móviles; [día 2 de enero 2010, hora 1:30pm] página en internet:

[http://www.tdr.cesca.es/TESIS_UPC/AVAILABLE/TDX-0319108 131609/01_padillaAguilar.pdf]

[8] Network Routing. Algorithms, Protocols, and Architectures. DEEPANKAR MEDHI, KARTHIKEYAN RAMASAMY.

[9] Nueva generación Protocolo de Internet, FACULTAD DE CIENCIA Y TECNOLOGIA ESCULA DE INFORMATICA, Trabajo de para optar el titulo de ingeniería sistema, 2004. Día 3 de marzo 2010, hora 5:30pm] página en internet:

[http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf]

[10] OPNET: Manual de usuario. Departamento de Ingeniería Telemática. Universidad Politécnica de Cataluña. 2004.

ANEXOS

MANUAL DE PRÁCTICAS DE LABORATORIO

AUTORES:

SORANYELI MANCERA MEZA

JENNY MARCELA ARDILA CRUZ

JHON JAIRO PADILLA

Practica N. 1

TITULO: TUNNEL MANUAL Y TUNNEL IPSEC

OBJETIVOS

- Entender el funcionamiento básico de Opnet Modeler referente a IPv6 en uno de los mecanismos de transición como es en tunnel manual, para comprender el envìo de paquetes.
- Analizar la configuración de protocolo RIP (Routing Information Protocol).
- Comprender la tabla de enrutamiento que presenta cada router, los destinos, rutas, fuentes de tráfico y configuraciones de los diferentes componentes de la red.
- Analizar el comportamiento en la red del túnel configurado de forma IPSEC y los componentes de seguridad que maneja en la cabecera de IPv6.

1. MARCO TEÓRICO

Algunos conceptos básicos para comprender con éxito la práctica.

RIP: Routing Information Protocol (Protocolo de encaminamiento de información). Calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancia.

El enrutamiento es la tarea de encontrar un camino desde un emisor a un deseado destino. En el período de investigación "El modelo de Internet" se reduce principalmente a una cuestión de encontrar una serie de routers entre la fuente y las redes de destino. Mientras un mensaje o datagrama permanece en una sola red o subred, los problemas son el reenvío, la responsabilidad de la tecnología que es específica a la red.[13]

[13] RFC 1058, Routing Information Protocol, Junio 1988

RIPng: (RIP próxima generación) es un protocolo de información de enrutamiento para el IPv6. Tiene por objeto permitir que los routers intercambiar información para rutas de computación a través de una red basada en IPv6. Cada router que implementa RIPng se supone que tiene una tabla de enrutamiento. Esta tabla tiene una entrada para cada destino que sea accesible todo el sistema operativo RIPng.[14]

Sistema de transición de IPv4 a IPv6

Hoy en día existen mecanismos que pueden ser implementados por host y routers IPv6 para mantener la compatibilidad con IPv4 los cuales agilizan la expansión de IPv6 en Internet y facilitan la transición. La clave para una transición exitosa a IPv6 es la compatibilidad con IPv4.

Los mecanismos están diseñados para ser empleados por host y routers IPv6 que necesitan interactuar con host IPv4 y que utilizan la infraestructura de enrutamiento de IPv4.[15]

Tunnel manual: Los mecanismos de transición se basan en encapsular dos redes IPvX que se encuentran separadas, con una red IPvy. En este caso se conectaràn dos redes IPv6 mediante una IPv4.[16]

[14] RFC 2080, RIPng for IPv6, enero 1987

[15] Implementación de Tuneles para IPv6 en Router Cisco; Marcelo J. Martínez Vallecillo, Felix Eduardo Sobalvarro Rojas,Jorge Luis Espinoza Lira

[16] IPv6 mecanismos de transición IPv4 a IPv6, Carlos Ralli Ucendo, http://www.cu.ipv6tf.org/pdf/carlos_ralli_transitiontutorial.pdf

Loopback: El dispositivo de red loopback es un interfaz de red virtual que siempre representa al propio dispositivo independientemente de la dirección IP que se le haya asignado. El valor en IPv4 es 127.0.0.0 y ::1 para el caso de IPv6.

La definición de los siguientes términos corresponde a OPNET.

Next hop address (dirección del siguiente salto): Devuelve la dirección IP del siguiente salto. Este método se utiliza para recuperar la dirección IP de la interfaz a la que va hacer enviado el paquete en el próximo salto**.**

Next hop node (nodo del siguiente salto): Es el nodo que tiene una interfaz con la dirección del siguiente salto.

Outgoing Interface (Interfaz de salida): Devuelve el nombre de la interfaz en el nodo de la fuente que se utiliza para llegar al siguiente salto. Se utiliza este método para recuperar el nombre de la interfaz en el nodo de la fuente que se utiliza para llegar al siguiente salto específico

Metric: Medida de la preferencia de una ruta. Normalmente, la métrica más baja es la ruta preferida. Si hay varias rutas a una red de destino dada, se utiliza la ruta con la métrica menor. Algunos algoritmos de enrutamiento solamente almacenan una única ruta para cualquier identificador de red en la tabla de enrutamiento,

aunque existan varias rutas. En este caso, el enrutador utiliza la métrica para determinar qué ruta debe almacenar en la tabla de enrutamiento. [17]

IPSEC: IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6.

2. DESCRIPCIÓN DEL ESCENARIO

Un router de una red tiene que ser capaz de determinar cuál de sus puertos de salida es el más apropiado para enviar un paquete en función de la dirección de destino. El router toma esta decisión a partir de una tabla de Encaminamiento. El problema fundamental del enrutamiento es: ¿Como rellenan los routers sus tablas de reenvió?. Los algoritmos de enrutamiento se encargan de construir las tablas de reenvió. El problema básico esta en encontrar el camino de menor costo entre dos nodos cualesquiera, donde el costo de un camino es igual a la suma de los costos de todos los tramos que lo componen. El enrutamiento se consigue en la mayoría de las redes ejecutando una serie de protocolos entre los nodos. Estos protocolos forman un algoritmo distribuido capaz de resolver el problema de encontrar el camino de menor costo en presencia de averías de nodos y enlaces o cambios en los costes de los diferentes tramos. Una de las clases principales de algoritmos de enrutamiento es el algoritmo vector-distancia. En él, cada nodo construye un vector que contiene las distancias (costos) a todos los otros nodos y distribuye ese vector a sus vecinos más próximos. El protocolo RIP es el ejemplo canónico de un protocolo de enrutamiento construido con base en este algoritmo. Los routers que ejecutan RIP envían sus anuncios de actualización regularmente (por ejemplo, cada 30 segundos). Un router también envía un mensaje de

[17] Tablas de Enrutamiento, Microsoft TechNet, http://technet.microsoft.com/es-es/library/cc737560(WS.10).aspx

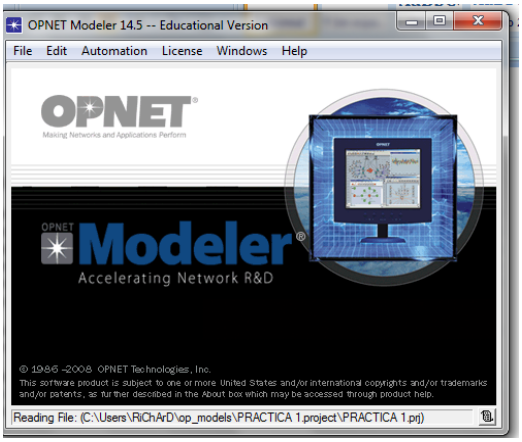
actualización cada vez que una actualización desde otro nodo le haga cambiar su tabla de encaminamiento.

El escenario planteado en esta práctica de laboratorio se compone de 2 redes que estarán conectadas mediante una nube IPv4. Para ello dos routers hacen la interconexión, uno en Bogotá y otro en Bucaramanga; estos enrutadores no se encuentran directamente conectados ya que se enlazan a una red trocal (IPv4). Esta práctica contiene temas como: RIP (protocolo de encaminamiento de información) y RIPNG (el protocolo de información de enrutamiento de próxima generación) y configuración de la aplicación PING.[18]

3. PASOS A SEGUIR

Ejecutar el programa como se muestra en la figura 1.1

Figura 1.1. Interfaz de OPNET



[18] **OPNET: Practica de laboratorio**, Protocolos de enrutado, Departamento de Ingeniería Telemática. Universidad Politécnica de Valencia.

3.1 Creación de un nuevo proyecto: Vaya a la opción **File** de la barra de herramientas y selecciones la opción **New**. A continuación aparecerá una ventana donde se solicita el tipo de proyecto. Seleccione la opción **Project** y luego haga click en **OK**. (**Descripcion rápida:** File→ New→ Project → ok).

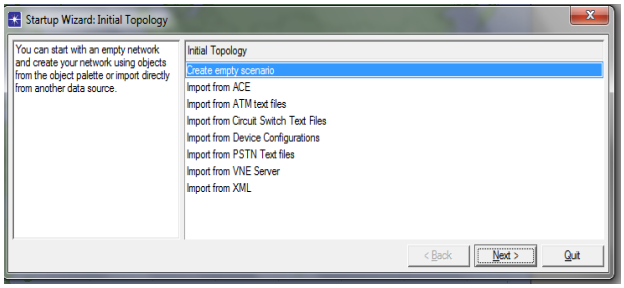
Project name → <TUNNEL_MANUAL>

Scenario name→ TUNNEL_SIN_CONFIGURAR→ok.

Asegúrese de que se encuentre seleccionada la opción **starup wizard.**

3.2 Configuración del escenario: a continuación aparecerá la figura 1.2, que muestra la ventana inicial del ayudante. Seleccione: (Startup wizard: initial topology → create empty scenario→ next).

Figura 1.2. Startup wizard initial topology



A continuación aparece la opción de selección de la escala de la red: (choose from maps→ next).

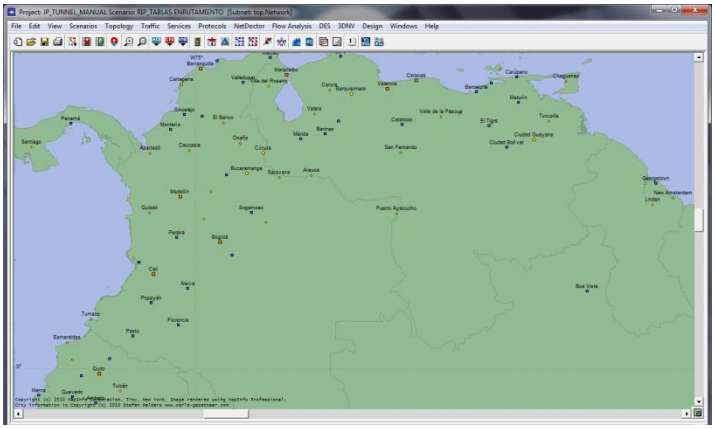
Se debe seleccionar el país en el que se va trabajar, en este caso no se selecciona ningún país (None→ next).

Ahora aparece el menú de tecnologías disponibles y seleccione **Internet_toolbox**: (select Technologies→ Internet_toolbox→next→Finish).

Aparece el mapa del mundo; ubíquese en Colombia, haciendo click izquierdo y movimiento scroll al mismo tiempo. Haga esta operación hasta que se ubique en

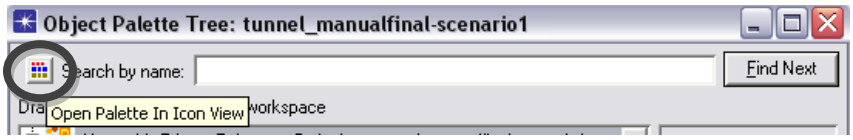
Colombia como se muestra en la figura 1.3. Con este escenario vacío ahora se procede a crear las estaciones.

Figura 1.3. Escenario



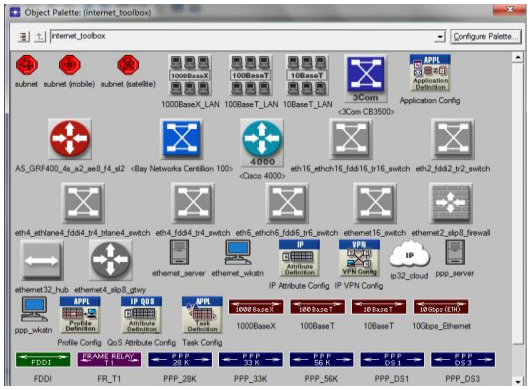
3.3 Creación del escenario de red: Diríjase a la barra de herramientas y haga click en el icono  **Object Palette Tree,** como se muestra en la figura 1.4; seleccione: **Open Palette In Icon View**

Figura 1.4. Object Palette Tree



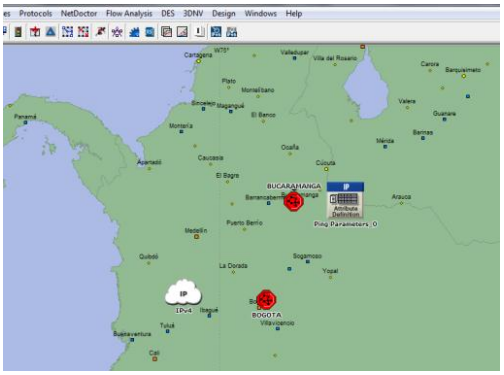
Allí se desplegaràn los iconos como se muestran en la figura 1.5, de los diferentes dispositivos de la tecnología usada.

Figura 1.5. Elementos de la red



Ahora, agregue dos elementos de tipo **Subnet**, uno en Bogotá y el otro en Bucaramanga. Además agregar una red de tipo nube **ip32 cloud** y también agregue un elemento de tipo **IP Attribute Config** que se encuentra la paleta; cabe aclarar que la subnet toma como nombre nodo 0, este debe ser cambiado oprimiendo click derecho sobre el objeto y picando en **Edit Attribute.** Colocar el nombre de la ciudad a la que corresponde, así como el nombre **Ping parámetros** al objeto **IP Attribute Config**. Además ponga el nombre IPv4 a la nube. El escenario deberá de quedar como la figura 1.6 manera:

Figura 1.6. Escenario Tunnel Manual



3.4 Creación y configuración de los elementos de la Subnet Bogotá: ahora se creará la red interna de la Subnet; para ello, en el icono de **Bogotá** se realiza doble click y se encontrará un espacio vacío en el cual se creará la red. Abra nuevamente el menú **Object Palette Tree** y seleccione los siguientes iconos de la tabla 1.1.

Tabla 1.1. Elementos de la subred Bogotá

Cantidad	Iconos
2	ethernet_wkstn
2	ethernet 16_ switch
2	ethernet_server
1	ethernet4_slip8_gtwy

Autores

A continuación edite los nombres de cada dispositivo como se muestra en la tabla1.2; oprimiendo click derecho sobre cada icono y seleccionando la opción **Set name**:

Tabla1.2 Nombre de los elementos de la subred Bogotá

Modelo	Nombre
ethernet_wkstn	wkstn A
ethernet_wkstn	wkstn B
ethernet server	server C
ethernet server	server D
ethernet 16_ switch	switch 1
ethernet 16_ switch	switch 2
ethernet4_slip8_gtwy	gateway

Autores

Una los diferentes elementos con enlaces de tipo **link model 100BaseT** (este se encuentra en el menú **object palette tree).** Conéctelos como se muestra en la tabla 1.3, de la siguiente manera:

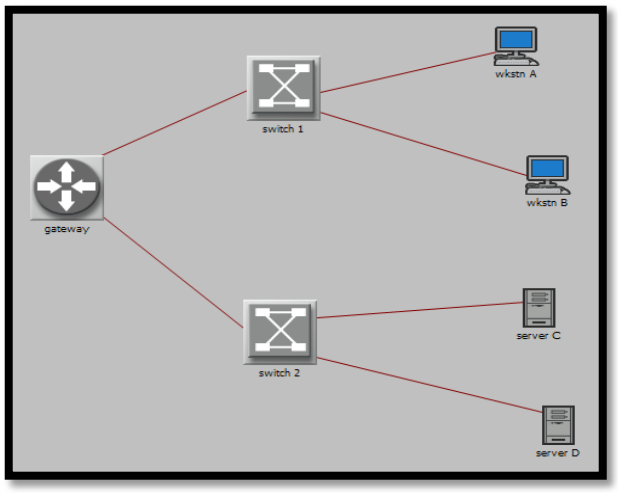
Tabla1.3. Conexiones de la subred Bogotá

Origen	Destino
switch 1	gateway
gateway	switch 2
wkstn A	switch 1
wkstn B	switch 1
server C	switch 2
Server D	switch 2

Autores

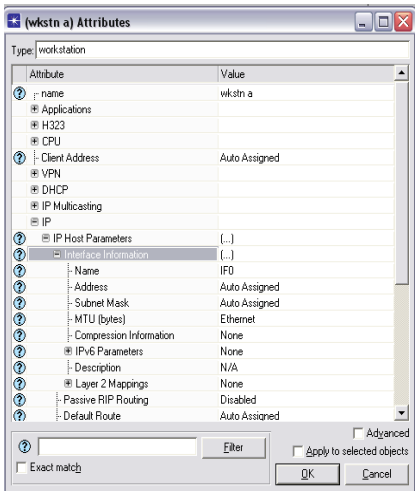
La red debe quedar como se observa en la figura 1.7.

Figura 1.7. Topología jerárquica Subred Bogotá



Ahora se procede a configurar cada elemento de la **Subnet de Bogotá**; ubíquese en **wkstn A,** realice click derecho, seleccione **editt atrributes**; ahí encontrará información de la estación. Los cambios que se harán son para indicar: dirección, submáscara y el protocolo a utilizar; esto se hace desplegando la opción **IP** luego **IP Host Parameters,** posteriormente abra la opción **Interface Information** como se muestra en la figura 1.8.

Figura 1.8. Atributos de la Subred Bogotá, wkstn A



En esta tabla de atributos se modifica:

- **Address,** oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne un nueva dirección IP por 192.0.2.3
- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne 255.255.255.0

Además en **IPv6 Parameters** oprimiendo click sobre el icono (+) se modificara algunos parámetros:

- **Link Local Address** en la opción asigne **Default EUI-64**
- **Global Address (es)** despliegue el icono (+), y encontrara la opción **Not Active,** cambie la opción **Address** que está en **Not Active,** en el menú **edit** por **3FFE:FFFF:D::2**, y **Address Type** debe estar **Non EUI-64**

- **IP Host Parameters** en la opción **IPv6 Default Route** que se encuentra en **Auto Assigned,** se asigna la dirección **3FFE:FFFF:D::1**
  Por último oprima **OK** para guardar los cambios realizados.

Este paso se repite para todas las estaciones tipo **wkstn** y las estaciones tipo **server** pero cada una tiene asignado diferentes valores en los parámetros como se muestra en la tabla 1.4.

Forma rápida de configuración:

- **IP→ IP Host Parameters→ Interface Information:** se usa para cambiar los paràmetros; Address y Subnet Mask
- **IP→ IP Host Parameters→ Interface Information→ IPv6 Parameters**: se utilize para cambiar los paràmetros; Link Local Address, Global Address (es)(Address,Address Type).
- **IP→ IP Host Parameters→ IPv6 Default Route**

Tabla1.4. Configuración de los elementos de la subred Bogotá

	wkstn B	**server C**	**server D**
Address	192.0.2.2	192.0.1.3	192.0.1.2
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Link local address	Default EUI-64	Default EUI-64	Default EUI-64
Global address (es) **Address:** **Address Type:**	3FFE:FFFF:D::3 Non EUI-64	3FFE:FFFF:E::2 Non EUI-64	3FFE:FFFF:E::3 Non EUI-64
IPv6 Default Route	3FFE:FFFF:D::1	3FFE:FFFF:E::1	3FFE:FFFF:E::1

Autores

Por último se asigna la dirección al GATEWAY**,** para ello, realice click derecho sobre este elemento, seleccione **edit atrributes**, desplegué **IP,** luego abra la opción **IP Routing Parameters,** ubíquese en **Interface Information (12rows)** y realice click en **(…)** aparecerá una tabla para editar las direcciones, que se encuentran en **Auto Assigned,** busque **edit** para colocar las nuevas direcciones y modifique lo siguientes parámetros como se muestra en la tabla 1.5.

Forma rápida de configuración:

- **IP→ IP Routing Parameters→ Interface Information (12rows):** Para cambiar Address y Subnet Mask

Tabla1.5. Configuración de los parámetros de Enrutamiento en puerta de enlace Subred Bogotá

	IF0	**IF1**	**IF10**
Address	192.0.2.1	192.0.1.1	192.0.5.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0

Autores

Luego oprima click en **OK,** para realizar cambios.

En la Puerta de enlace (Gateway), vuelva al menú de atributos, en **IP** desplegamos la opción **IP Routing Parameters**, en la línea de **Loopback Interface** oprima click en **(…).** Al oprimir click en **edit** aparece una ventana, y en la parte inferior **(rows)** agregue en la casilla el número 1, realice los siguientes cambios en la tabla oprimiendo click en la opción **edit** de cada casilla:

- Name: loopback
- Address: 192.0.7.1
- Subnet mask: 255.255.255.0
- Routing protocol(s): habilite el RIP

Para finalizar oprima **OK** en la tabla.

En la misma tabla de atributos de la puerta de enlace, en la opción **IP,** seguido de **IPv6 Parameters,** se encuentra **Interface information,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** que se encuentra en cero (0), edite el número 2.

- Abra la opción **IF0** y coloque lo siguiente; **Link local address** en **Default EUI-64,** además despliegue el menú oprimiendo en el icono (+)de en **Global Address (es)** oprima click en **(…)** busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit,** coloque **3FFE:FFFF:D::1,** para finalizar oprima **OK.**
- Luego abra la otra opción **IF0**, y donde se encuentra **Name** en **IF0**, busque **IF1** y colóquelo, automáticamente cambia el nombre.

  Posteriormente en la opción **Link local address** en **Default EUI-64,** además en **Global Address (es**) oprima click en **None,** busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit,** coloque **3FFE:FFFF:E::1,** para finalizar oprima **OK.** Finalizamos oprimiendo click en **OK** para guardar cambios en la ventana principal de **Gateway Attributes.**

Vuelva a la red principal oprimiendo click derecho en el fondo de la ventana y elija **Go to the Parent Subnet**.

3.5 Creación y configuración de los elementos de la Subnet Bucaramanga: ahora se creará la red interna de la Subnet; para ello, en el icono de **Bucaramanga** se realiza doble click y se encontrará un espacio vacío en el cual se creará la red. Abra nuevamente el menú **Object Palette Tree** y seleccione los iconos de la tabla 1.6.

Tabla 1.6. Elementos de la subred Bucaramanga

Cantidad	Iconos
4	ethernet_wkstn
2	ethernet 16_ switch
1	ethernet4_slip8_gtwy

Autores

A continuación edite los nombres de cada dispositivo como se muestra en la tabla 1.7; oprimiendo click derecho sobre cada icono y seleccionando la opción **Set name**:

Tabla 1.7. Nombres de los elementos de la subred Bucaramanga

Modelo	Nombre
ethernet_wkstn	wkstn A
ethernet_wkstn	wkstn B
ethernet_wkstn	wkstn C
ethernet_wkstn	wkstn D
ethernet 16_ switch	switch 1
ethernet 16_ switch	switch 2
ethernet4_slip8_gtwy	gateway

Autores

Una los diferentes elementos con enlaces de tipo **link model 100BaseT** (este se encuentra en el menú **object palette tree).** Conéctelos como se muestra en la tabla 1.8 de la siguiente manera.

Tabla 1.8. Conexiones de la subred Bucaramanga

Origen	Destino
switch 1	gateway
Switch 1	gateway
wkstn A	switch 1
wkstn B	switch 1
wkstn C	switch 2
wkstn D	switch 2

Autores

La red debe quedar como se observa en la figura 1.9.

Ahora se procede a configurar cada elemento de la **Subnet de Bucaramanga.**

Ubíquese en **wkstn A,** y realice click derecho, seleccione **editt atrributes**; ahí encontrará información de la estación. Los cambios que se harán son para indicar: dirección, submáscara y el protocolo a utilizar; esto se hace desplegando la opción **IP** luego **IP Host Parameters,** posteriormente abra la opción **Interface Information** como se muestra en la figura 1.10.

Figura 1.9. Topología jerárquica Subred Bucaramanga

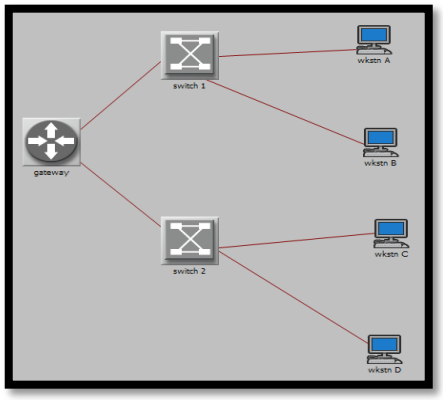
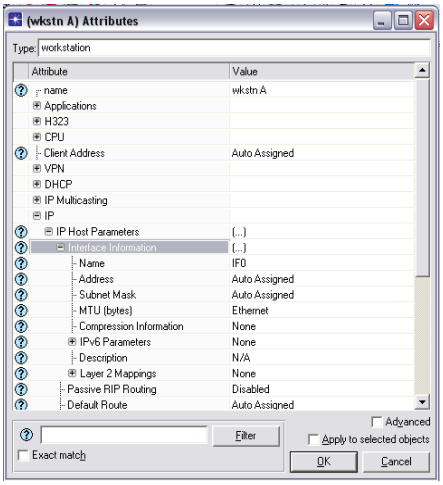


Figura 1.10. Atributos de la Subred Bucaramanga, wkstn A



En esta tabla se modifica:

- **Address,** oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne un nueva dirección IP por **192.0.4.3**
- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne 255.255.255.0

Además en **IPv6 Parameters** oprimiendo click sobre el icono (+) se modificara algunos parámetros:

- **Link Local Address** en la opción asigne **Default EUI-64**
- **Global Address (es)** despliegue el icono (+), y encontrarà la opción **Not Active,** cambie la opción **Address** que está en **Not Active,** en **edit** por **3FFE:FFFF:A::2**, y **Address Type** debe estar **Non EUI-64**
- **IP Host Parameters** en la opción **IPv6 Default Route** que se encuentra en **Auto Assigned,** se asigna la dirección **3FFE:FFFF:A::1**

  Por último oprima **OK** para guardar los cambios realizados.

Este paso se repite para todas las estaciones tipo **wkstn** pero cada una tiene asignado diferentes valores en los parámetros como se muestra en la tabla 1.9.

Forma rápida de configuración:

- **IP→ IP Host Parameters→ Interface Information:** Se usa para cambiar los parámetros; Address y Subnet Mask
- **IP→ IP Host Parameters→ Interface Information→ IPv6 Parameters**: Se utiliza para cambiar los parámetros; Link Local Address, Global Address (es)(Address,Address Type).
- **IP→ IP Host Parameters→ IPv6 Default Router**

Tabla1.9. Configuración de los elementos de la subred Bucaramanga

	wkstn B	**wkstn C**	**Wkstn D**
Address	192.0.4.1	192.0.3.1	192.0.3.2
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
Link local address	Default EUI-64	Default EUI-64	Default EUI-64
Global address (es) **Address:** **Address Type:**	3FFE:FFFF:A::3 Non EUI-64	3FFE:FFFF:B::2 Non EUI-64	3FFE:FFFF:B::3 Non EUI-64
IPv6 Default Route	3FFE:FFFF:A:1	3FFE:FFFF:B::1	3FFE:FFFF:B::1

Autores

Por último, se asigna la dirección a la puerta de enlace GATEWAY; para ello, realice click derecho sobre este elemento, seleccione **edit atrributes**, desplegué **IP,** luego abra la opción **IP Routing Parameters,** ubíquese en **Interface Information (12rows)** y realice click en **(…)** aparecerá una tabla para editar las direcciones, como se muestra en la tabla 1.10.

Forma rápida de configuración:

- **IP→ IP Routing Parameters→ Interface Information (12rows):** Para cambiar Address y Subnet Mask.

Tabla1.10. Configuración de los parámetros de orden físico y sub-interfaz en la puerta de enlace, Subred Bucaramanga

	IF0	**IF1**	**IF10**
Address	192.0.4.2	192.0.3.3	192.0.6.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0

Autores

Luego oprima click en **OK.**

En la puerta de enlace GATEWAY, vuelva al menú de atributos, en **IP** desplegamos la opción **IP Routing Parameters**, en la línea de **Loopback Interface** oprima click en **None.** Al oprimir click en **edit** aparece una ventana, en la parte inferior **(rows)** agregue en la casilla el número 1, realice los siguientes cambios en la tabla oprimiendo en la opción **edit** de cada casilla:

- Name: loopback
- Address: 192.0.8.1
- Subnet mask: 255.255.255.0
- Routing protocol(s): habilite el RIP

Para finalizar oprima en la tabla **OK.**

En la misma tabla de atributos de la puerta de enlace, en la opción **IP,** seguido de **IPv6 Parameters,** se encuentra I**nterface information,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** que se encuentra en cero (0), edite el número 2.

- Abra la opción **IF0** y coloque lo siguiente, **Link local address** en **Default EUI-64,** además despliegue el menú oprimiendo en el icono (+)de **Global Address (es)** y oprima click en **(…)** busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit,** coloque **3FFE:FFFF:A::1,** para finalizar oprima **OK.**
- Luego abra la otra opción **IF0**, y donde se encuentra **Name** en **IF0**, busque **IF1** y colóquelo, automáticamente cambia el nombre. Posteriormente en la opción **Link local address** en **Default EUI-64,** además en Global Address (es) oprima click en **None,** busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit,** coloque **3FFE:FFFF:B::1,** para finalizar oprima **OK.** Finalice oprimiendo click en **OK** en la ventana principal de los atributos de la puerta de enlace **(Gateway Attributes).**

3.6 Visualización de la tabla de reportes: para visualizar la tabla de enrutamiento debe seleccionar el elemento GATEWAY de cada Subnet, hacer click derecho sobre él, escoger **edit attributes**, buscar la opción **Reports,** desplegar **IP Forwarding Table** que se encuentra con **Do Not Export,** inmediatamente busque ahí la opción **Export at End Simulation,** y oprimía **OK**

para realizar cambios. Realice este mismo procedimiento con la GATEWAY de Bucaramanga.

3.7 Configuración de Ping: Para la configuración de Ping, se realizan los siguientes pasos:

Ingrese a la Subnet de Bogotá, abra **Object Palette Tree** y seleccione **ip_ping_traficc** para hacer las siguientes conexiones:

- Conecte **Wkstn A** de la Subnet de **BOGOTA**, realizando click derecho en el área de trabajo y seleccione **Go To Parent Subnet**, inmediatamente haga doble click en la Subnet Bucaramanga y conéctela con el **wkstn B.**

- Conecte **Wkstn B** de la Subnet **BOGOTA**, realizando click derecho en el área de trabajo y seleccione **Go To Parent Subnet,** inmediatamente haga doble click en la Subnet Bucaramanga y se conéctela con **wkstn D**.

- Conecte **Wkstn A** de la Subnet **BUCARAMANGA,** realizando click derecho en el área de trabajo y selecciones **Go To Parent Subnet,** inmediatamente haga doble click en la Subnet Bogotá y se conéctela con el **server D.**

- Conecte **Wkstn C** de la Subnet **BUCARAMANGA**, realizando click derecho en el área de trabajo y seleccione **Go To Parent Subnet**, inmediatamente haga doble click en la Subnet Bogotá y se conecta con el **server C.**

Ahora bien, la subred Bogotá queda como la figura 1.11 y la subred Bucaramanga como la figura 1.12

Figura 1.11. Subred Bogotá

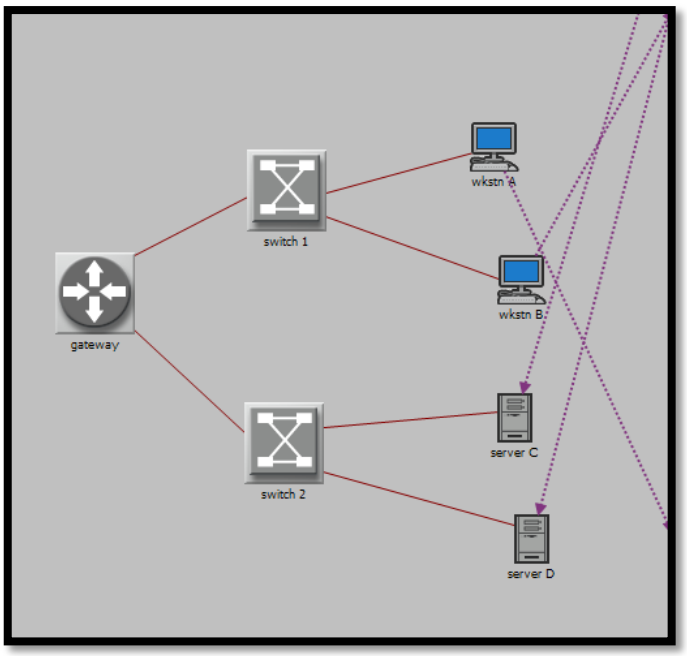
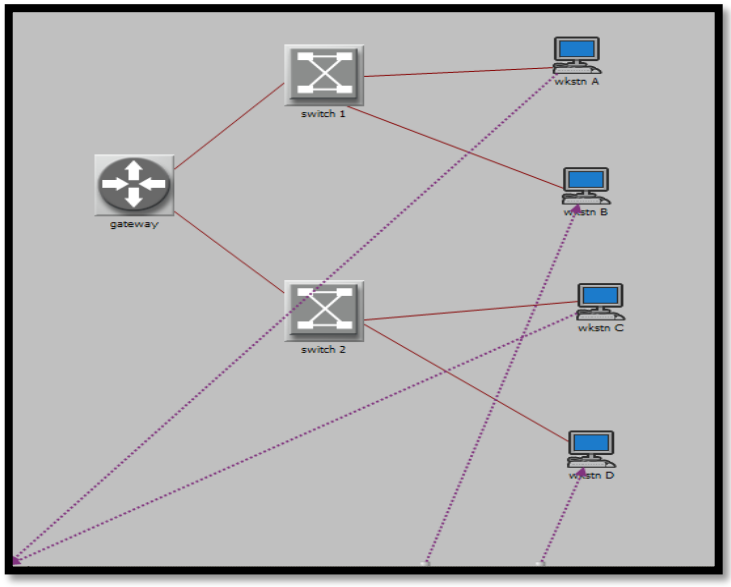


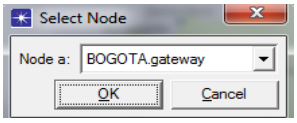
Figura 1.12. Subred Bucaramanga



3.8 Creación de los enlaces Nube IPv4 - Routers: Se continúa con los enlaces entre la nube **IPv4** y los **routers**. Regrese al escenario principal e ingrese al menú de elementos **object palette tree** y seleccione el icono de enlace **PPP_DS3**.

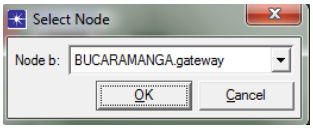
- Proceda a enlazar **Bogotá - IPv4** y se seleccione **Nodo a: BOGOTA.gateway**, como se muestra en la figura 1.13

Figura 1.13. Nodo a Bogota.gateway



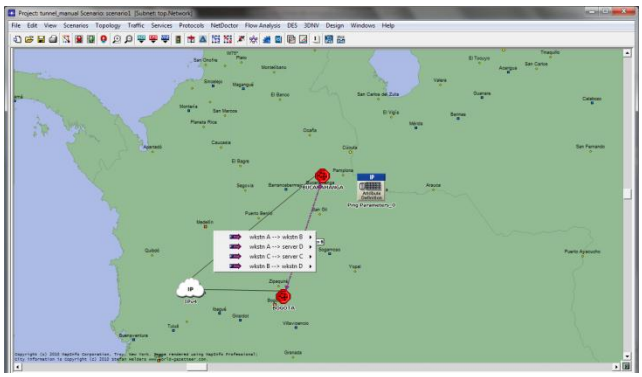
- Ahora enlace **IPv4 - Bucaramanga** y seleccione **Nodo b: BUCARAMANGA.gateway**, como se muestra en la figura 1.14

Figura 1.14. Nodo b Bucaramanga.gateway



De acuerdo con las conexiones anteriores se crea el enlace entre Bogotá y Bucaramanga, como se muestra en la figura 1.15

Figura 1.15. Enlace Bogotá-Bucaramanga



3.9 Configuración del Loopback: Dado que la **nube IPv4** está en la red y ayuda a interconectar una Subnet con la otra, se debe configurar el **loopback**. Se realiza click derecho sobre la nube IPv4 seleccionando **edit attributes,** ahí se despliega una serie de parámetros, escoja **IP**, abra las opciones para seleccionar **IP Routing Parameter,** busque **Loopback Interfaces** que se encuentra con la opción **None,** haga click sobre esta y busque **edit** para crear una fila. Se abrirá la ventana **Loopback Interfaces Table** y proceda a editar el número 1 **(rows)**, se modificaran los siguientes parámetros.

- Name: loopback
- Address: 192.0.7.1
- Subnet mask: 255.255.255.0
- Routing protocol: habilite el RIP

Para finalizar oprima **OK** en la ventana principal de **IPv4 Attributes.**

3.10 Selección de resultados: En el escenario principal, realice click derecho, seleccione la opción **Choose individual DES statistics,** seleccione lo siguiente como se mustra en la tabla 1.11.

Tabla1.11. Selección de resultados

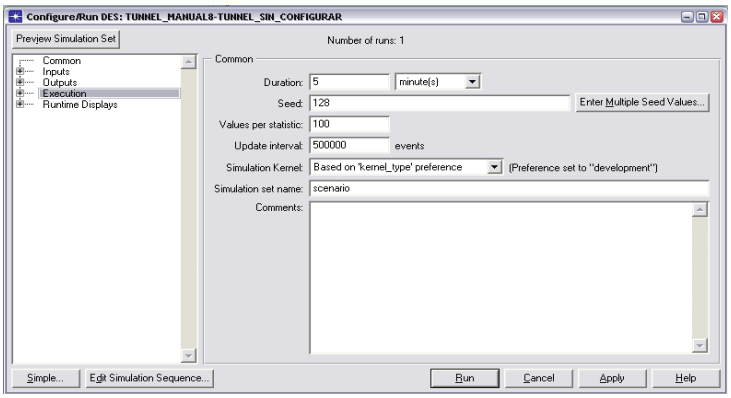
Link Statistics
• **Point-to-point**
✓ throughput (bits/sec)→
✓ throughput (bits/sec)←
✓ throughput (packets/sec)→
✓ throughput (packets/sec)←

Autores

3.11 Realización de simulación: Para llevar a cabo la simulación, realice los siguientes pasos:

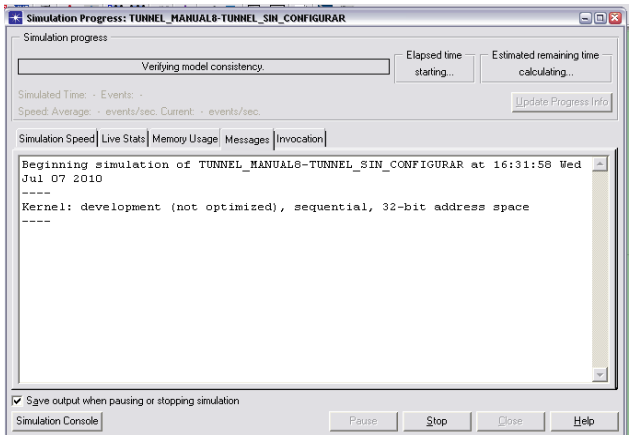
- En la barra de herramientas se encuentra el icono RUN  donde aparece una ventana mostrando la duración de la simulación como se muestra en la figura 1.16; esta duración se puede modificar para ver mayores intervalos de tiempo. Asigne los siguiente; Duration 5 minutos, seed 128, values per statistics 100, Update interval 100000

Figura 1.16. Parámetros para la simulación



Después de configurar estos parámetros, haga click en **RUN** y se observarà como se muestra en la figura 1.17

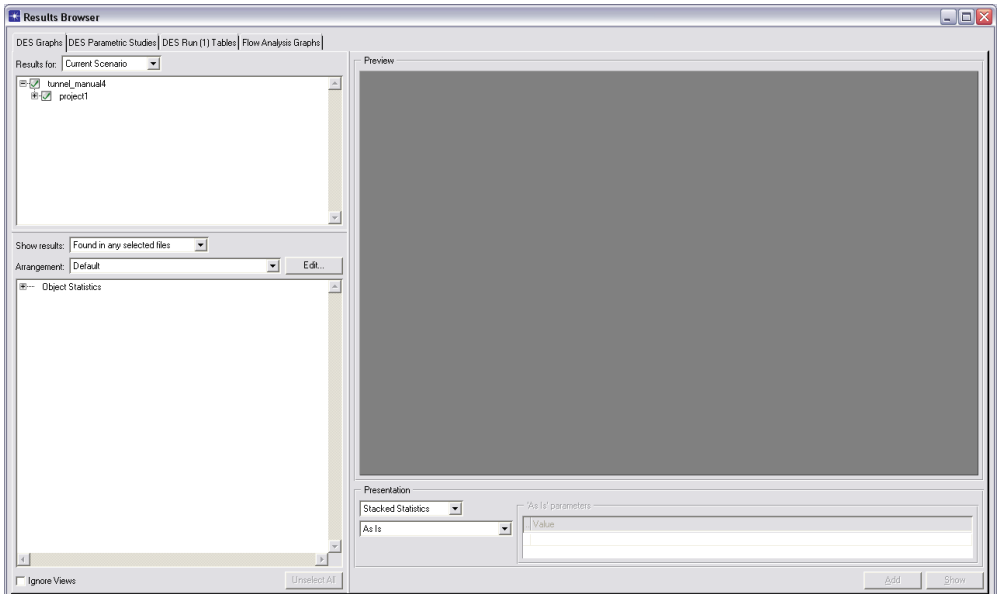
Figura 1.17. Detección de errores



De esta manera al terminar el proceso de detección de errores se cierra la ventana en el botón **close**.

3.12 Resultados Tunnel manual sin configurar: para revisar la tabla de resultados se ingresa al menú **Flow Analysis,** posteriormente se buscara **Results** y se dará click en **View Results**, aparecerá la figura 1.18, ventana (**Result Browser)**, donde se debe ingresar a la pestana **DES Graphs.**

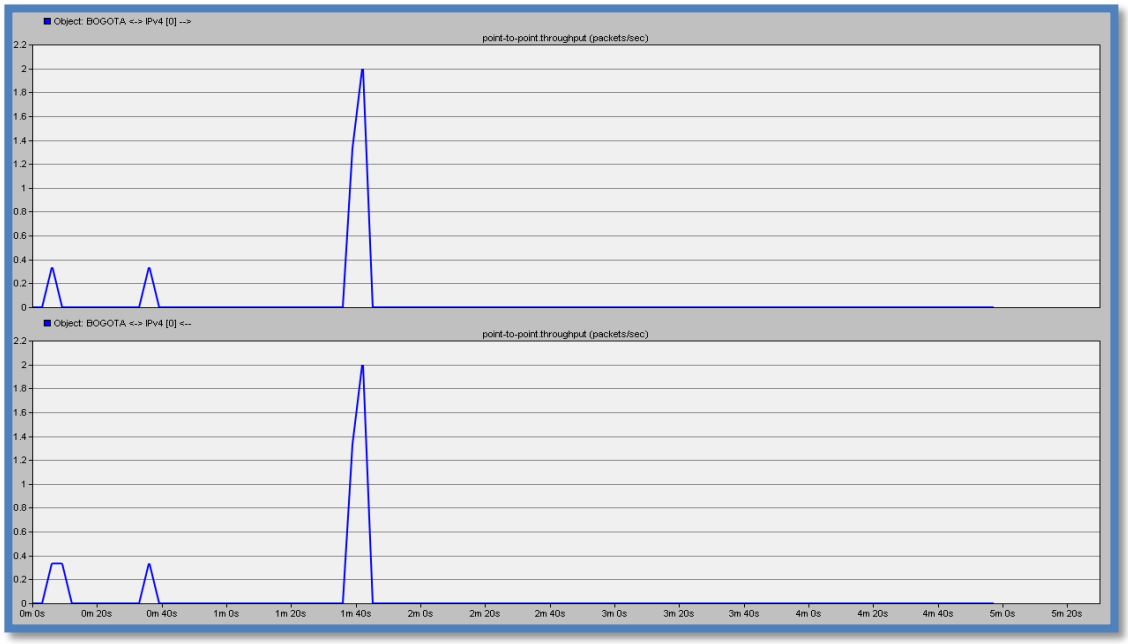
Figura 1.18. Resultados del navegador



Para lograr observar este rendimiento individual, **sin configurar el Tunnel Manual**, se realizan los siguientes pasos, en la parte inferior izquierda sale el menú **Object Statistics→ Bogotá<->IPv4** hasta encontrar **point-to-point**, seleccione **throughput (packets /sec)→** y **throughput (packets/sec)←,** Con estas gráficas se logra observar que efectivamente se esta transmitiendo y recibiendo tráfico de Bogotá – IPv4.

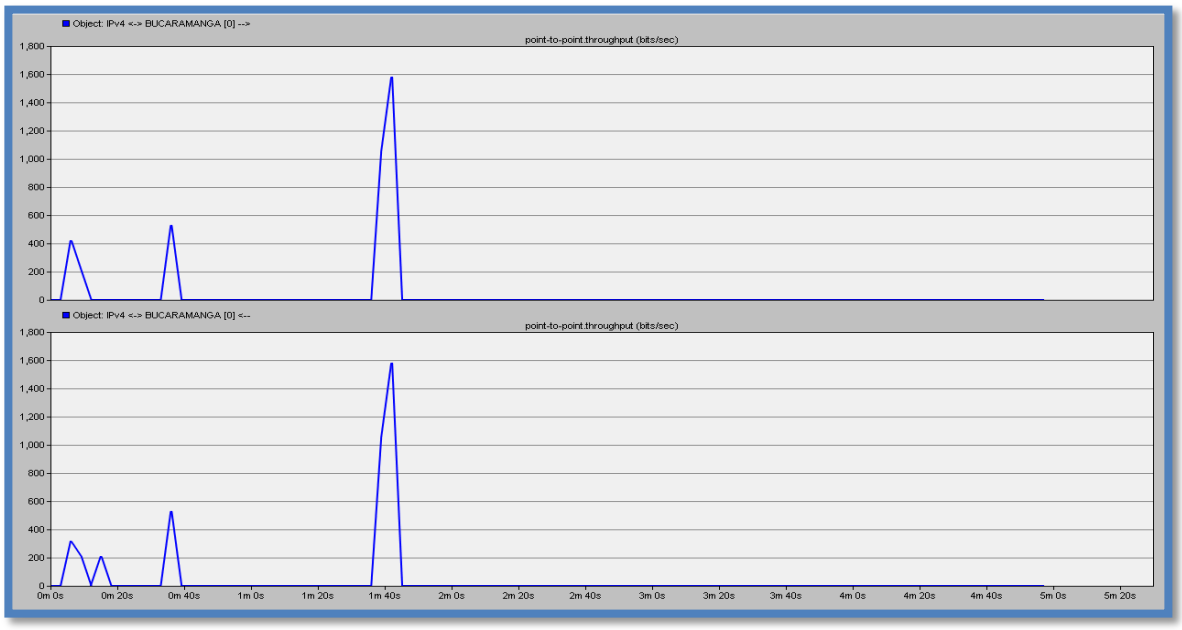
Para visualizar las gráficas de una mejor forma, realice click en la opción **show,** donde aparecerá una ventana con las dos gráficas, realice click derecho sobre la parte gris, y busque la opción **Time Axis,** asigne el valor **Auto-scale,** para poder observar la línea de tiempo en el cual fueron simuladas.

Bogotá – IPv4 (packets/sec)



Object Statics→ Bucaramanga→ IPv4<->Bucaramanga hasta encontrar **point-to-point y** seleccione **throughput (bits /sec)→** y **throughput (bits /sec)←.** Con estas gráficas se logra observar que efectivamente se está transmitiendo y recibiendo tráfico de IPv4-Bucaramanga.

IPv4-Bucaramanga (bits/sec)



En la misma figura 1.17, en la parte superior seleccione la pestaña **DES Run (1) Tables,** y despliegue la opción **Object Tables,** posteriormente abra todos los menú que hay, hasta encontrar la opción **Performance**, oprima click sobre **IP Forwarding Table at End of Simulation** y **IPv6 Forwarding Table at 300 seconds,** allí saldrán las figura 1.19 y 1.20, encontrara una serie de características que hicieron parte de la simulación, se mostraràn la de la Subnet Bogotá.

TABLA DE ENRUTAMIENTO

En la tabla de IP Forwarding (Reenvió IP) se pueden observar los parámetros de encaminamiento por los que se reenvía el tráfico IP. En esta tabla se proporciona una lista de rutas IP para las direcciones IP de destino seleccionadas, incluidas las rutas IP que se definen de manera dinámica. Las rutas IP se basan en máscaras de red, próximos saltos, métrica y protocolos de reenvío. Estos parámetros

determinan cómo se reenvían o eliminan paquetes específicos. Cuando se configura una dirección IP en una interfaz, se incluye en la tabla de reenvío IP.

Las tablas de enrutamiento consisten en encontrar la mejor ruta para la transferencia de información.[19]

Figura 1.19. IP Forwarding table at end of simulation Bogotá *sin configurar*

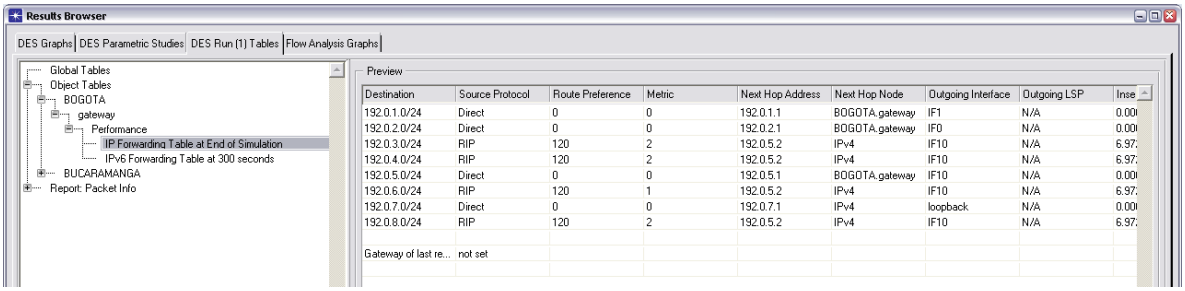
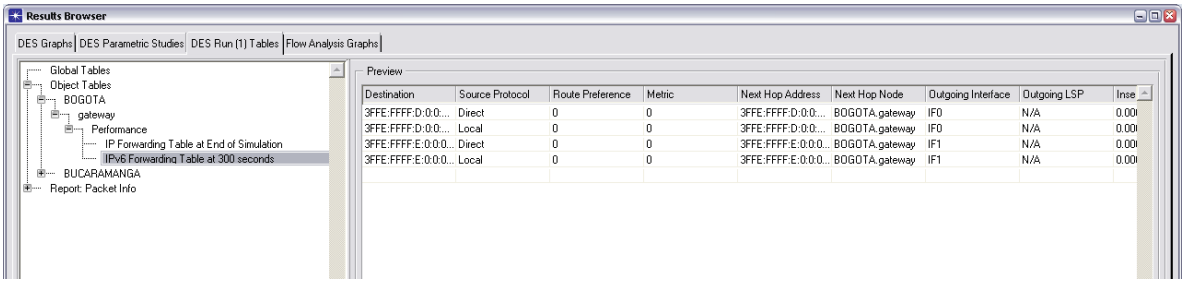


Figura 1.20. IP Forwarding table at 300 seconds Bogotá sin configurar



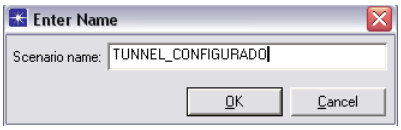
En las tablas de enrutamiento se encuentran datos importantes del escenario como el recorrido que hace cada paquete para llegar a su destino.

***NOTA:** Como se ha podido Observar en ningún paso se ha configurado el **tunnel manual,** que hace de mecanismo de transición para envió de información entre redes IPv4 e IPv6, por esta razón en la tabla de enrutamiento no aparece el Tunnel Manual. Para solucionar esto se realiza lo siguiente.*

[19] Configuración del Encaminamiento, DELL, http://docs.us.dell.com/support/edocs/network/pc6024/sp/ug/configuf.htm

3.13 Creación de un nuevo escenario: vaya al menú **Scenarios,** seleccione **Duplicate Scenario,** allí saldrá la figura 1.21 donde se asignara el nombre de **TUNNEL_CONFIGURADO**

Figura 1.21. Scenario Name

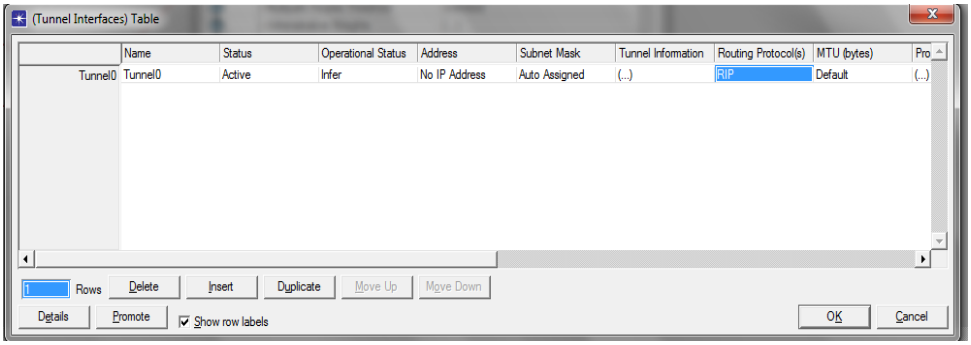


Oprima **OK** para finalizar, se duplicara el escenario, si quiere regresar al escenario anterior que se llama **TUNNEL_SIN_CONFIGURAR,** regrese al menú **Scenarios,** diríjase **Switch To Scenario,** allí aparecerán los dos escenarios que se crearon.

3.14 Configuración de mecanismo de transición en la puerta de enlace: En **TUNNEL_CONFIGURADO,** se ingresa a la **Subnet de Bogotá**, luego ubíquese en el **Gateway** haciendo click derecho sobre él, escoja la opción **Edit Attributes,** despliegue el menú **IP,** y busque **IP Routing Parameters,** donde se encuentra la opción **Tunnel Interfaces** que viene configurado con el valor **none;** haga click en **edit,** a continuación saldrá la figura 1.22.

En la parte inferior de la tabla **Tunnel Interface** se encuentra la opción **rows;** agregue una nueva fila colocando esta opción en 1.

Figura 1.22 Tunnel Interfaces



En la misma tabla en la opción **Tunnel Information,** que viene asignado con la opción **<Not Set>,** se debe oprimir y buscar **edit**, se abrirá una ventana **(Tunnel Information) Table,** donde asignarà lo siguiente:

- Tunnel source: IF10
- Tunnel destination: 192.0.6.1
- Tunnel mode: IPv6 (Manual)
- Passenger protocol(s): IPv6

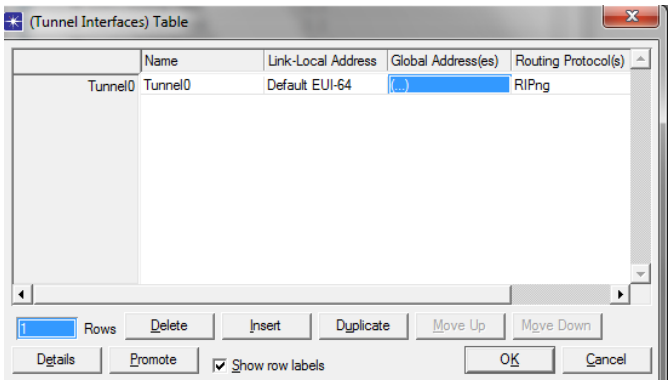
Finalice oprimiendo en **OK** en la ventana de los **atributos** para que guarde los cambios realizados.

Después de haber realizado esto, se notarà que se ha configurado el **Tunnel Manual** porque aparece un nueva interfaz de túnel en la opción **IP Routing Protocols→RIP Parameters→Tunnel Interface (1 Row);** se observara que se creó un **Tunnel Manual.**

En la misma puerta de enlace GATEWAY**,** despliegue el menú **IP** busque **IPv6 Parameters,** donde se encuentra la opción **Tunnel Interfaces** que se encuentra configurada con el valor **none;** haga click en **edit,** a continuación saldrá una ventana **(Tunnel Interfaces table).**

En la parte inferior de la tabla **Tunnel Interface** se encuentra la opción **rows;** agregue una nueva fila colocando esta opción en 1. Como se muestra en la figura 1.23.

Figura 1.23 Tunnel Interfaces IPv6



Modifique lo siguiente:

Link local address, que se encuentra en **Not Active** se debe asignar **Default EUI-64**. **Global address** que esta con la opción **None**, se debe oprimir en **edit,** donde aparece una nueva ventana, oprima click en la parte superior donde se encuentra **Address,** saldrá en la parte inferior la opción **Insert,** oprima allí, se activaran unas nuevas opciones, luego en **Address** que esta con **Not Active** se debe buscar **edit** y colocar el siguiente valor **3FFE:FFFF:C::2,** en **Address Type** coloque la opción **Non EUI-64** y finalice oprimiendo **OK.**

En **Routing protocol(s)** debe estar habilitado el **RIPng**, posteriormente haga click en **OK** en la ventana de los **Atributos.**

Realice este mismo proceso con la **Subnet de Bucaramanga** pero en la puerta de enlace (Gateway). Pero tenga en cuenta que los datos que serán modificados;

IP→ IP Routing Parameters → Tunnel Interfaces, oprima click en **None** y busque **edit** y agregue una fila **(1 Rows).** En la misma tabla en la opción **Tunnel Information,** que viene asignado con la opción **<Not Set>,** se debe oprimir y buscar **edit**, y se abrirá una ventana **(Tunnel Information) Table,** donde asignarà lo siguiente:

- Tunnel source: IF10
- Tunnel destination: 192.0.5.1
- Tunnel mode: IPv6 (Manual)
- Passenger protocol: IPv6

Oprima **OK** para guardar cambios, en la opción **Routing protocols** debe estar habilitado el **RIP**, finalice oprimiendo click en **OK.** Posteriormente haga click en **OK** en la ventana principal de los **Attributes,** para guardar cambios.

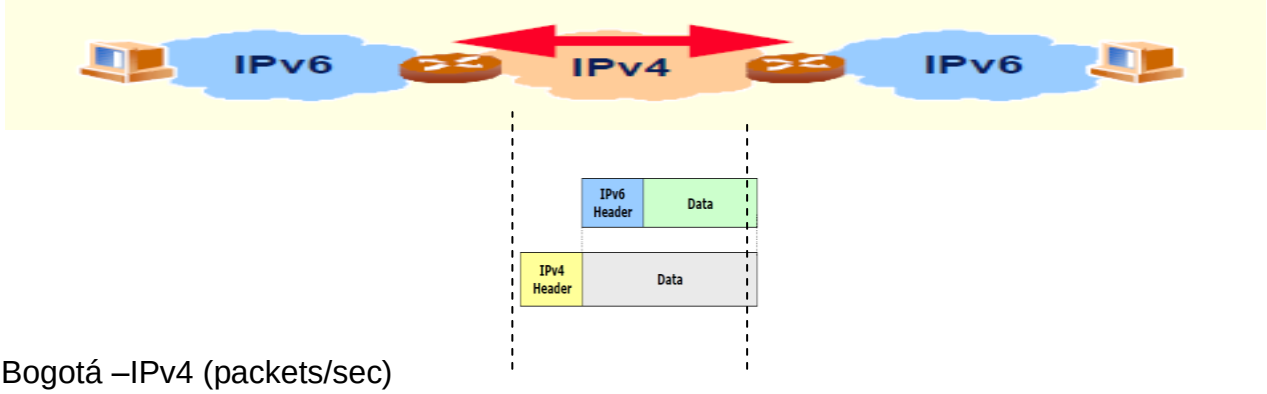
Después de haber realizado esto, se notarà que se ha configurado el **Tunnel Manual** porque aparece un nueva interfaz de túnel en la opción **IP Routing Protocols→RIP Parameters→Tunnel Interface (1 Rows);** se observarà que se creó un **Tunnel Manual,** para finalizar este proceso haga click en el botón **OK** de la ventana principal de atributos del **GATEWAY.**

Para finalizar se configura un último **tunnel**, oprimiendo click derecho sobre la **subnet de Bucaramanga**, escogiendo la opción **Edit Attributes.** Despliegue el menú **IP,** busque **IPv6 Parameters,** donde se encuentra la opción **Tunnel Interfaces** que se encuentra configurada con el valor **none;** haga click en **edit,** a continuación saldrá un ventana (**Tunnel Interfaces table).** En la parte inferior de la tabla **Tunnel Interface** se encuentra la opción **row;** agregue una nueva fila colocando esta opción en 1. En esa tabla se debe modificar lo siguiente;

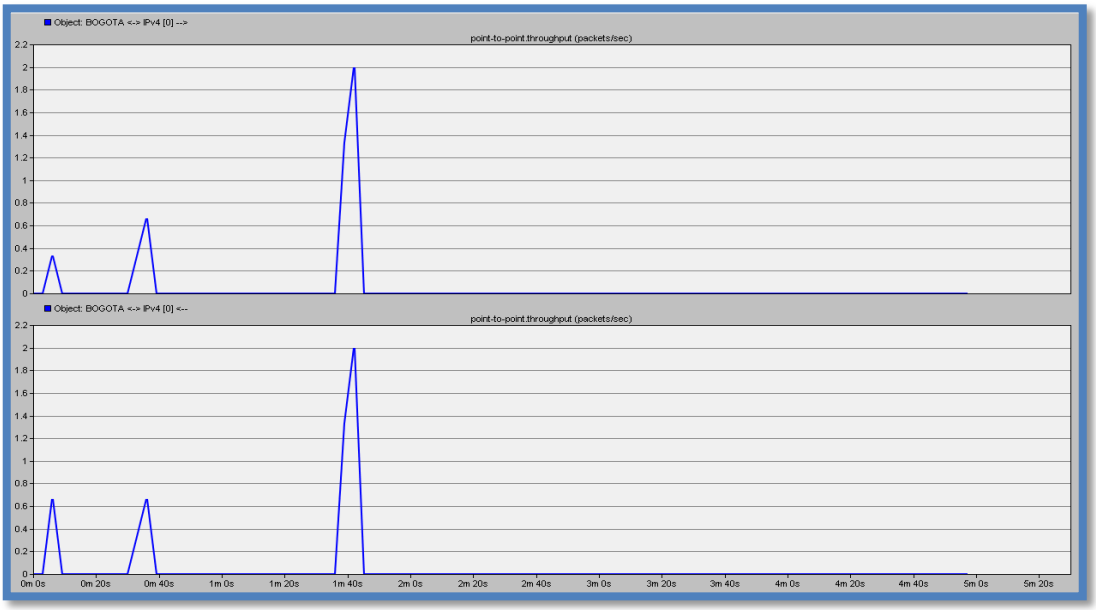
Link local address, que se encuentra en **Not Active** se debe asignar **Default EUI-64**. **Global address** que esta con la opción **None**, se debe oprimir en **edit,** donde aparecerá una nueva ventana y se oprima click en la parte superior donde se encuentra **Address,** saldrá en la parte inferior la opción **Insert,** oprima allí, se activaran unas nuevas opciones, luego en **Address** que esta con **Not Active** se debe buscar **edit** y colocar el siguiente valor **3FFE:FFFF:C::1,** en **Address Type** debe estar en la opción **Non EUI-6,** finalice oprimiendo **OK.**

En **Routing protocol(s)** debe estar habilitado el **RIPng**, posteriormente haga click en **OK** en la ventana de los **Attributes.**

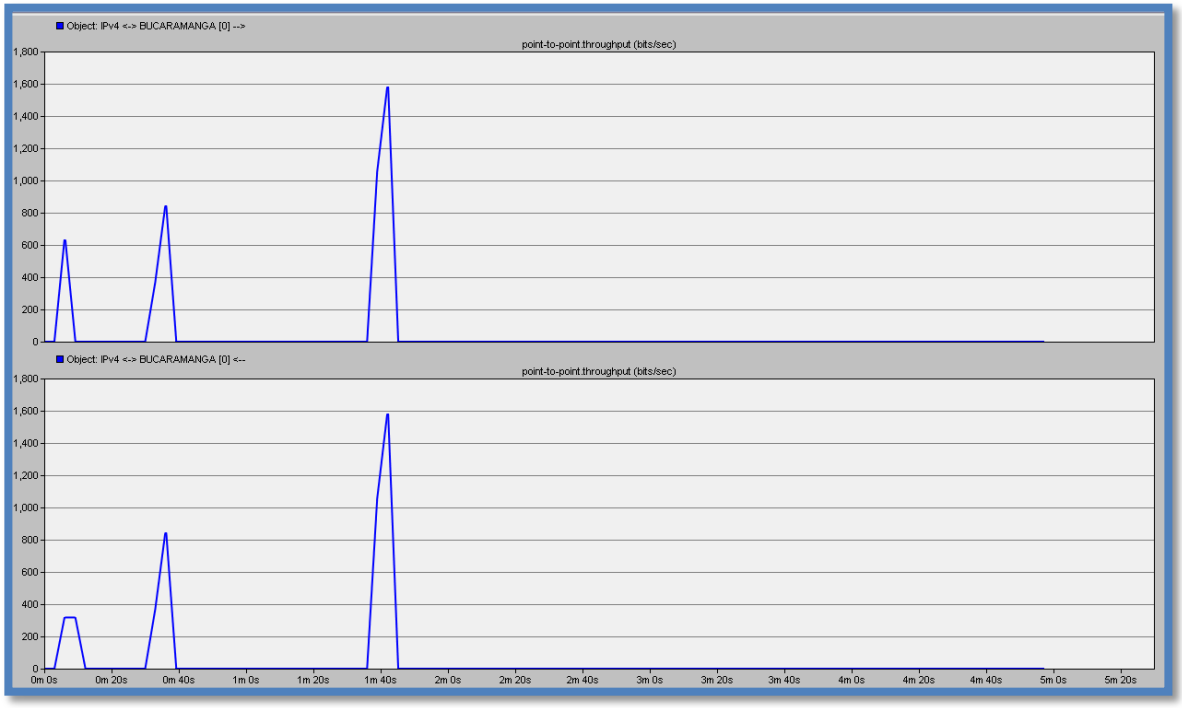
3.15 Resultados Tunnel Manual configurado: después de los pasos anteriores vuelva a correr la simulación con los mismos parámetros de la simulación anterior. Obtendrá gráficos como los siguientes o similares. (El ancho de banda aumenta debido a que los datagramas IPv6 se encapsulan sobre datagramas IPv4 para atravesar redes). En las graficas se observa que aumenta el ancho de banda en pequeña proporción.



Bogotá –IPv4 (packets/sec)



IPv4-Bucaramanga (bits/sec)



TABLAS DE ENRUTAMIENTO

Figura 1.24. IP Forwarding table at end of simulation *Bogotá configurado*

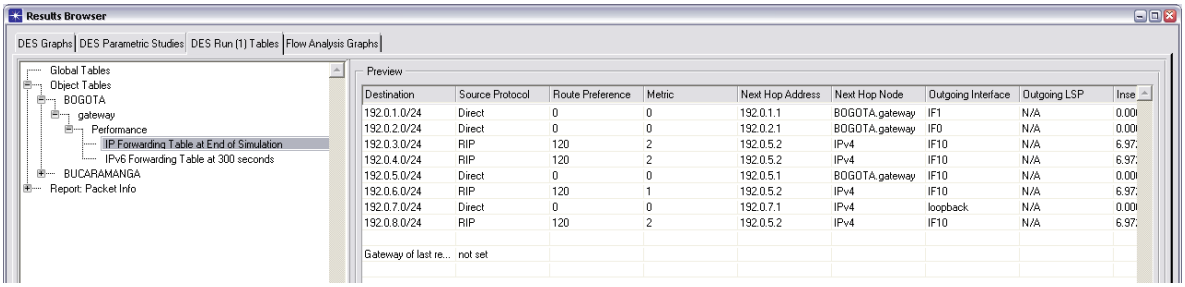
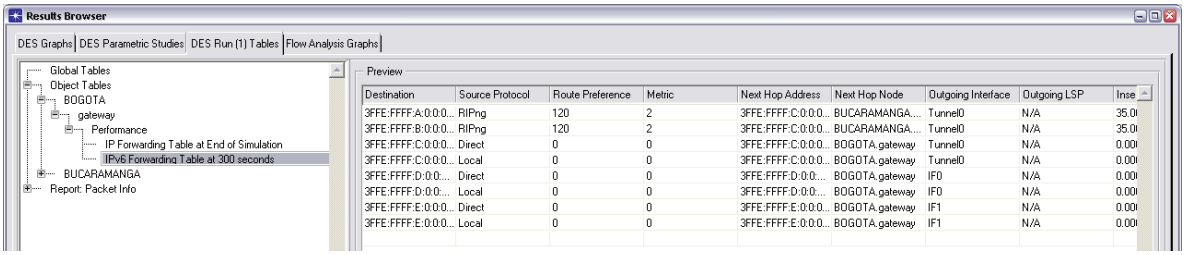
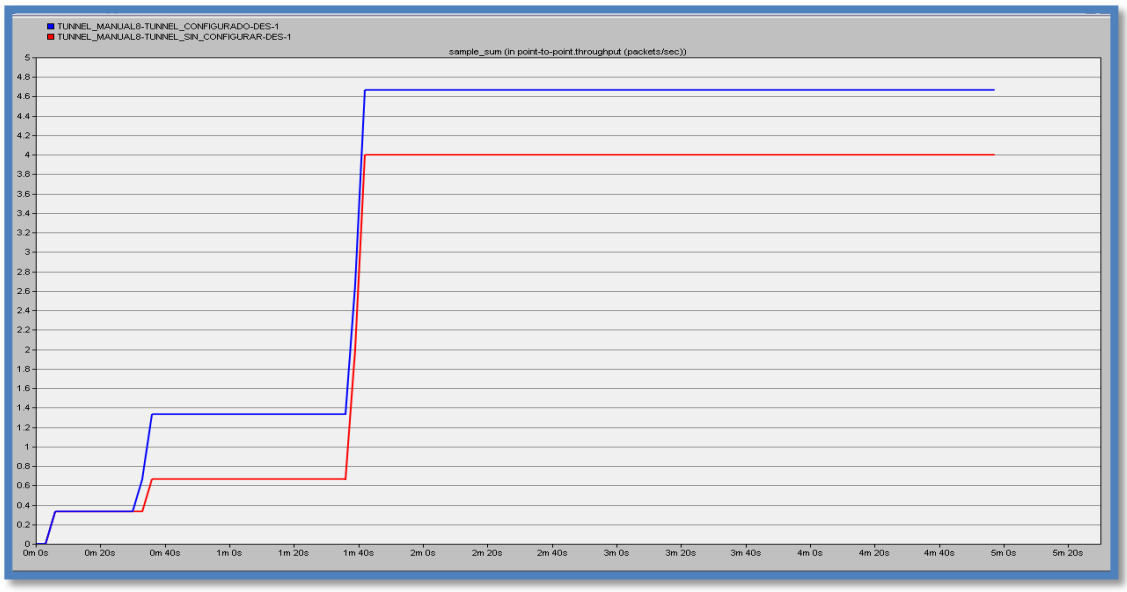


Figura 1.25. IP Forwarding table at 300 seconds Bogotá configurarado

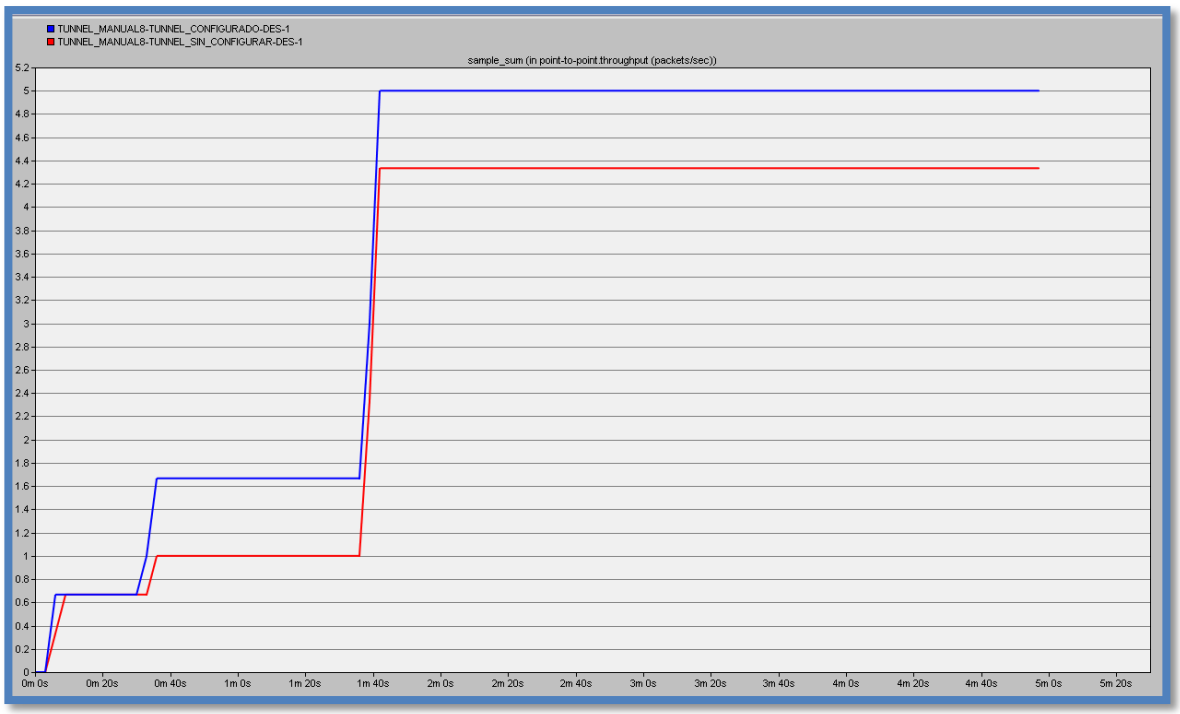


3.16 Comparaciones: Para realizar una comparación entre **Tunnel_sin_configurar** y **Tunnel_configurado**, y se logre observar con exactitud el desarrollo de la práctica, se debe hacer lo siguiente; estando en el ùltimo escenario **(TUNNEL_CONFIGURADO)** en la ventana **Result Browser**, se debe ingresar a la pestaña **DES Graphs.** Seleccione **Current Project,** que se localiza en **Results for**, busque la opción **All Projects,** y señale las dos opciones **(Tunnel_sin_configurar , Tunnel_configurado)** , luego en **Object Statistics,** escoja **Throughput (packets/sec)-->** para BOGOTA <-> IPv4, después en la parte inferior de la ventana, donde dice **Presentation,** buscar **Overlaid Statistics,** y donde dice **As Is** buscar **Sample Sun** (hace la suma de los paquetes que van llegando). En la siguiente gràfica se observa que el ancho de banda aumenta.

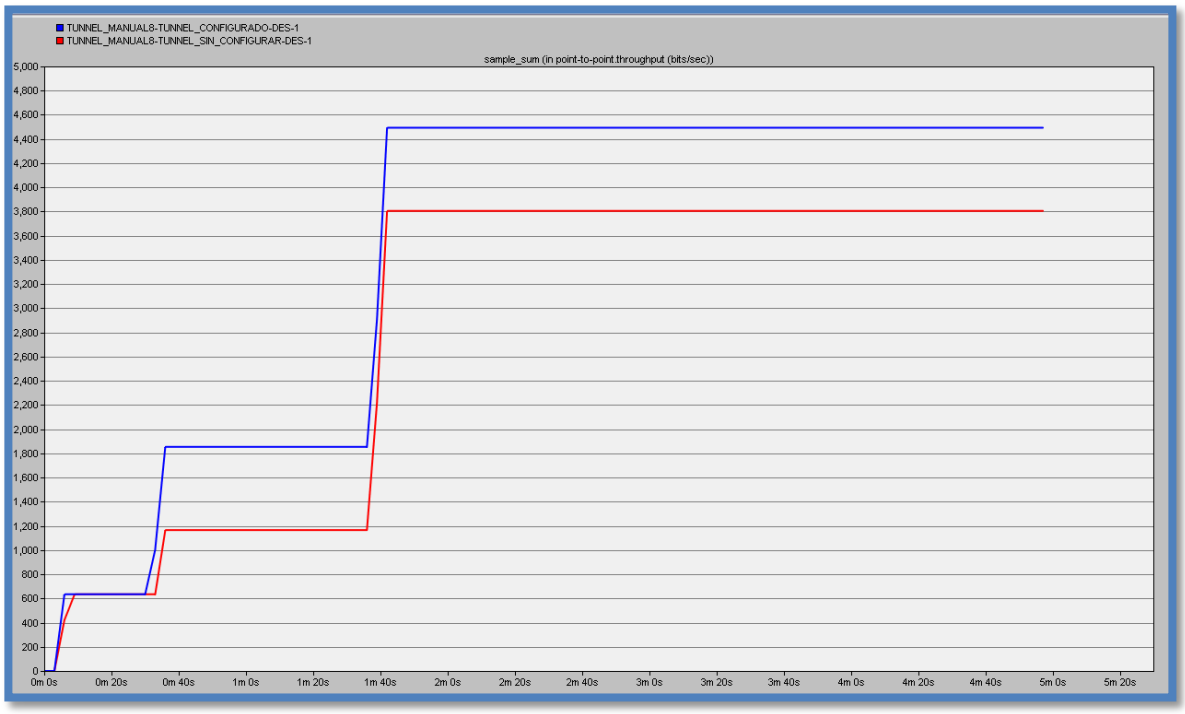
Bogotà<->IPv4 Throughput (packet/sec) - ->



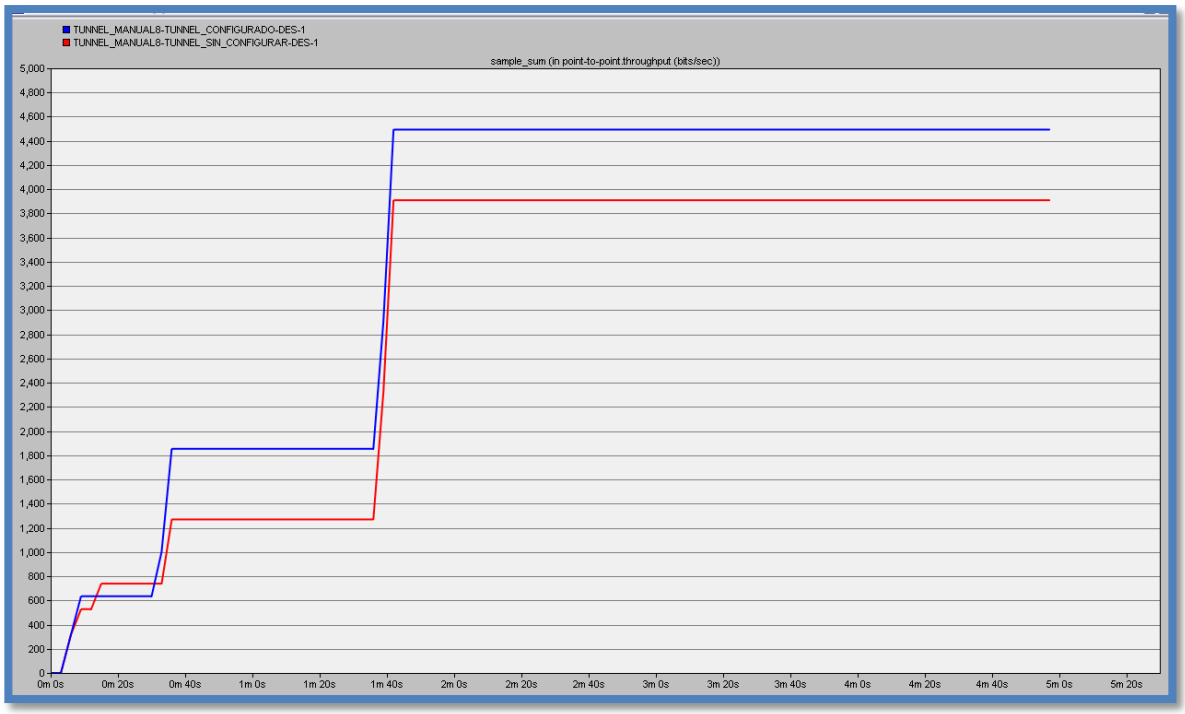
Bogotà<->IPv4 Throughput (bits/sec) < - -



IPv4 <-> Bucaramanga Throughput (bits/sec) < - -

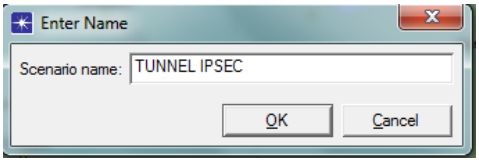


IPv4 <-> Bucaramanga Throughput (bits/sec) - ->



3.17 Creación de un nuevo escenario: vaya al menú **Scenarios,** seleccione **Duplicate Scenario,** allí saldrá la figura 1.21 donde se asignara el nombre de **TUNNEL_IPSEC**

Figura 1.26. Scenario Name



Oprima **OK** para finalizar, se duplicara el escenario, si quiere regresar los escenario a los escenarios creados, regrese al menú **Scenarios,** diríjase **Switch To Scenario,** allí aparecerán los tres escenarios que se crearon.

3.18 Configuración de mecanismo de transición en la puerta de enlace: En **TUNNEL_IPSEC,** se ingresa a la **Subnet de Bogotá**, luego ubíquese en el **Gateway** haciendo click derecho sobre él, escoja la opción **Edit Attributes,** despliegue el menú **IP,** y busque **IP Routing Parameters,** donde se encuentra la opción **Tunnel Interfaces,** haga click sobre (…) busque **edit,** a continuación saldrá la figura 1.22. En la parte inferior de la tabla **Tunnel Interface** se encuentra la opción **rows;** agregue una nueva fila colocando esta opción en 1.

En la misma tabla, en la opción **Tunnel Information,** que tiene asignado la opción **(…),** se debe oprimir y buscar **edit**, se abrirá una ventana **(Tunnel Information) Table,** donde asignara lo siguiente:

- Tunnel source: IF10
- Tunnel destination: 192.0.6.1
- Tunnel mode: IPsec
- Passenger Protocol(s): IPv6

Finalice oprimiendo en **OK** en la ventana de los **atributos** para que guarde los cambios realizados.

Después de haber realizado esto, se notara que se ha configurado el **Tunnel IPsec** porque aparece una nueva interfaz de túnel, ingresando en los atributos de la puerta de enlace (Gateway), en la opción **Security→IPSec Parameters→Tunnel Interface (1 Rows).**

Realice este mismo proceso con la **Subnet de Bucaramanga** pero en la puerta de enlace (Gateway). Pero tenga en cuenta que los datos que serán modificados; **IP→ IP Routing Parameters → Tunnel Interfaces,** oprima click en **(…),** y busque **edit.** En la misma tabla, en la opción **Tunnel Information,** que viene asignado con la opción **(…),** se debe oprimir y buscar **edit**, y se abrirá una ventana **(Tunnel Information) Table,** donde asignara lo siguiente:

- Tunnel source: IF10
- Tunnel destination: 192.0.5.1
- Tunnel mode: IPSec
- Passenger protocol: IPv6

Oprima **OK** para guardar cambios, realice el procedimiento anterior para verificar que se creo el túnel IPSec.

3.19 Visualización de los resultado: Para visualizar los resultados en la barra de herramienta en la opción **Scenarios →Manage Scenarios** se visualizan los tres escenarios creados, el tiempo de duración para los escenarios debe ser de **10 minutos**, para guarda los nuevos tiempos de simulación oprima click sobre **OK**, y corra la simulación para observar los nuevos gráficos.

Para revisar la tabla de resultados se ingresa al menú **Flow Analysis,** posteriormente se buscara **Results** y se dará click en **View Results**, aparecerá la ventana **(Result Browser)**, donde se debe ingresar a la pestana **DES Graphs.**

En la opción **Results For**, seleccione **Current Project,** y señale **TUNNEL_CONFIGURADO** y **TUNNEL_IPSEC.**

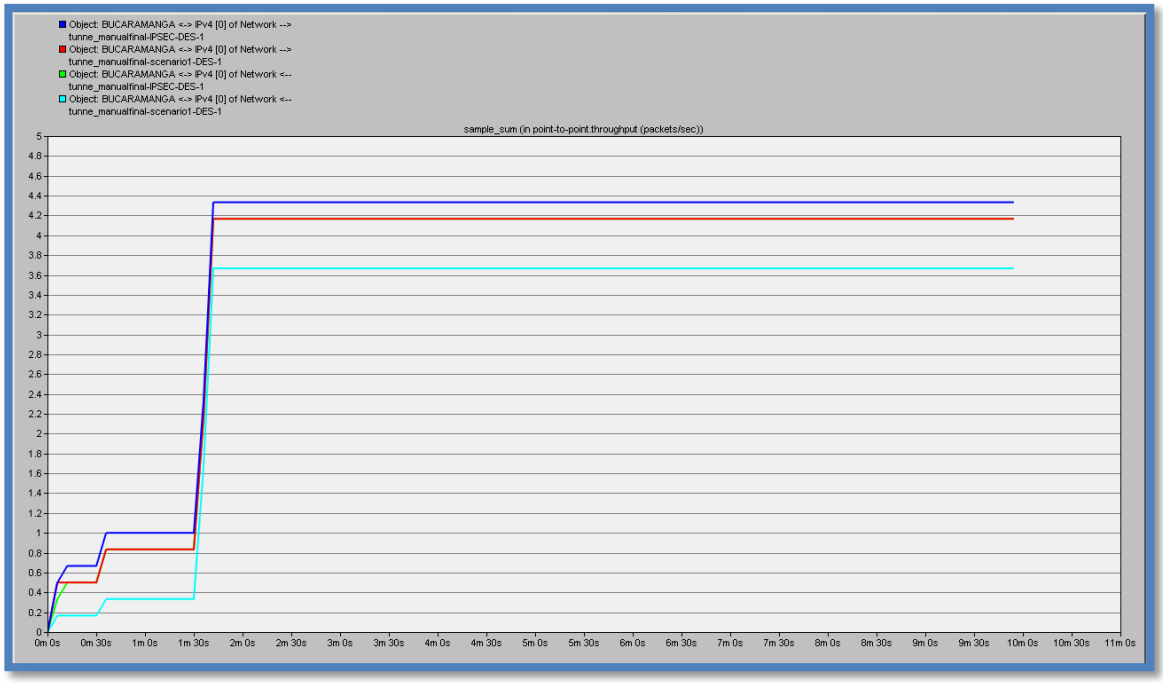
Después en la parte inferior de la ventana, donde dice **Presentation,** buscar **Overlaid Statistics,** y donde dice **As Is** buscar **Sample Sun** (hace la suma de los paquetes que van llegando). En la siguientes grafica se observa que el ancho de banda aumenta.

Bogota<->IPv4 Throughput (packets/sec) - ->

Bogota<->IPv4 Throughput (packets/sec)<- -

IPv4 <-> Bucaramanga Throughput (packets/sec) - ->

IPv4 <-> Bucaramanga Throughput (packets/sec) < - -



TAREA

- Para lograr observar otro comportamiento de la red, varié el tiempo de simulación aumentando o disminuyendo, observe y analice que sucede con las gráficas.

- Al realizar los dos escenarios Tunnel configurado y Tunnel sin configurar, se deben observar las tablas de enrutamiento y realizar comparaciones entre ellas y explique qué cambios se observan.

Practica N. 2

TITULO: 6TO4

OBJETIVOS

- Analizar la importancia del mecanismo de transición 6TO4 sobre redes IPv4 e IPv6.
- Comprender la tabla de enrutamiento que presenta cada router, los destinos, rutas, fuentes de tráfico, servicios y configuraciones de los diferentes componentes de la red.
- Permitir la coexistencia entre redes IPv4 e IPv6, a través de la configuración 6to4

1. MARCO TEÓRICO

6to4: Es uno de los mecanismos de transición de IPv4 A IPv6 que han sido propuestos por el IETF. EL 6to4 es un sistema que permite enviar paquetes IPv6 sobre redes IPv4 obviando la necesidad de configurar túneles manualmente. Fue diseñado para permitir conectividad IPv6 sin la cooperación de los proveedores de internet. Este mecanismo de transición es una forma de túneles router a router. Permite que dominios IPv6 aislados se comuniquen con otros dominios IPv6 con una mínima configuración.

Definiciones de palabras que se encontraran nuevas en esta práctica.

6bone: Ésta es la red virtual, un entorno de prueba IPv6 que los programadores y los proveedores de Internet pueden utilizar para desarrollar y ofrecer servicios

basados en IPv6 y adquirir la experiencia necesaria para implementar el nuevo protocolo. [20]

FTP (**F**ile **T**ransfer **P**rotocol - **Protocolo de Transferencia de Archivos**): Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor.[21]

Terminal Server: Servicios de Terminal son un componente de los sistemas operativos Windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red.[22]

HTTP: Hypertext Transfer Protocol o **HTTP** (protocolo de transferencia de hipertexto). Define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario).[23]

2. DESCRIPCIÓN DEL ESCENARIO

En este escenario se construyen dos sitios 6to4 en la red, uno que es sitio web **(6to4 sitio A)** y **(6to4 sitio C),** que se conectan a través de la red troncal IPv4, por medio de túneles 6to4 que se configuran en ambos routers A y C que les permite comunicarse entre sí. Las direcciones 6to4 del sitio A se crean a partir de la dirección IPv4 192.0.4.1 que es la dirección de la interfaz del router A, que conecta al IPv4 Backbone

---

[20] RFC 3956,Connection of IPv6 Domains via IPv4 Clouds,Enero 2001
[21] RFC 959, FILE TRANSFER PROTOCOL (FTP),Octubre 1985
[22] RFC 1091, Telnet Terminal-Type Option, Febrero 1989
[23] RFC 2616,Hypertext Transfer Protocol -- HTTP/1.1,Junio 1999

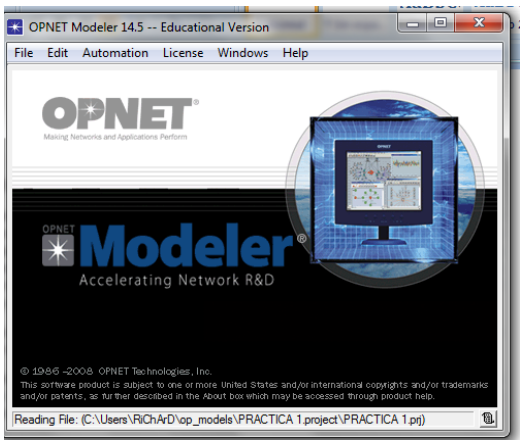
Para comunicarse con destinos non-6to4 IPv6, estos sitios utilizan un proveedor de servicios de servicios de Internet Relay en este caso es llamado (sitio B). Tanto los routers A como C tienen una ruta predeterminada al enrutador B. Así los paquetes que van desde un sitio de 6to4 (sitio A) a un sitio nativo IPv6 (Sitio D); serán primero encapsulados y enviados al router B por medio de túneles 6to4, en este sitio se desencapsulan y luego se envían al destinatario final.

En general la práctica mostrarà como resultado el tráfico enviado y recibido por la aplicación y la capa IP en varios nodos.[24]

3. PASOS A SEGUIR

Ejecutar el programa como se muestra en la figura 2.1

Figura 2.1. Interfaz de OPNET



3.1 Creación de un nuevo proyecto: Vaya a la opción **File** de la barra de herramientas y selecciones la opción **New**. A continuación aparecerá una ventana donde se solicita el tipo de proyecto. Seleccione la opción **Project** y luego haga click en **OK**. (**Descripción rápida:** File→ New→ Project → ok)

[24] **OPNET: Manual de Usuario**, Transicion de IPv4 a IPv6.

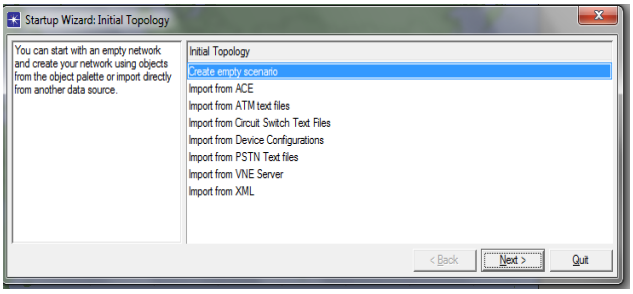
Project name → < 6TO4_TUNNEL >

Scenario name→ project 1→ok.

Asegúrese de que se encuentre seleccionada la opción **starup wizard.**

3.2 Configuración del escenario de la red: A continuación aparecerá la figura 2.2, que muestra la ventana inicial del ayudante. Seleccione: (Startup wizard: initial topology → create empty scenario→ next).

Figura 2.2. Startup wizard initial topology



A continuación aparece la opción de selección de la escala de la red: (office→ next).

Se debe seleccionar el espacio en cual se va trabajar:(Size→ X span 100, Y span 100, Unit Meters→ next)

Ahora aparece el menú de tecnologías disponibles y seleccione **Internet_toolbox y Ethernet advanced**: (select Technologies→ Internet_toolbox, Ethernet advanced →next→Finish).

3.3 Creación y configuración de la red: Aparece un espacio de trabajo en azul en el cual se crearà la topología; Diríjase a la barra de herramientas y haga click en el icono  **Object Palette Tree** como se muestra en la figura 2.3**;** seleccione: **Open Palette In Icon View**

Figura 2.3. Object Palette Tree

Allí se desplegaràn los iconos como se muestra en la figura 2.4, de los diferentes dispositivos de las tecnologías que se escogieron.

Figura 2.4. Elementos de la red

Ahora agregue los elementos que se encuentran en la tabla 2.1

Tabla2.1. Elementos de la red 6to4

Cantidad	Iconos
2	ethernet_wkstn_adv
4	ethernet4_slip8_gtwy
2	Ip32_cloud
1	ethernet_server_adv
1	ethernet_server
1	Application Config
1	Profile Config
1	IP Attribute Config

Autores

A continuación edite los nombres de cada dispositivo como se encuentra en la tabla 2.2; oprimiendo click derecho sobre cada icono y seleccionando la opción **Set name**:

Tabla2.2. Nombres de los elementos de la red 6to4

Modelo	Nombre
ethernet_wkstn_adv	wkstn A
ethernet_wkstn_adv	wkstn B
ethernet4_slip8_gtwy	Router A
ethernet4_slip8_gtwy	Router B
ethernet4_slip8_gtwy	Router C
ethernet4_slip8_gtwy	Router D
Ip32_cloud	IPv4 Backbone
Ip32_cloud	6bone
ethernet_server_adv	Terminal server
ethernet_server	Http server
Application Config	Applications
Profile Config	Profiles
IP Attribute Config	Ping Params

Autores

Para buscar otros objetos que se necesitan, Diríjase a la barra de herramientas y haga click en el icono  **Object Palette Tree,** saldrá una ventana y seleccione **Node Models**, despliegue esta opción hasta encontrar **Fixed Node Models** e ingrese a **By Name,** busque la carpeta **ppp***, seleccione cada

Icono (2 **ppp_server_adv** y 2 **ppp_wkstn_adv),** posteriormente llévelo hasta el área de trabajo.

Cambie los nombres por los de la tabla 2.3.

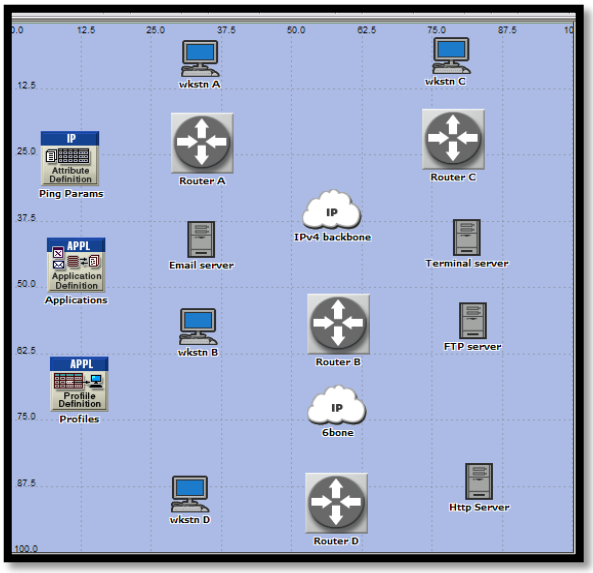
Tabla2.3. Nombres de otros elementos de la red 6to4

Modelo	Nombre
ppp_wkstn_adv	wkstn C
ppp_wkstn_adv	wkstn D
ppp_server_adv	Email server
ppp_server_adv	FTP server

Autores

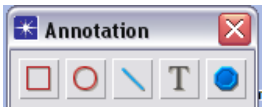
Ahora organice los elementos como se encuentra en la figura 2.5.

Figura 2.5. Escenario 6to4



Agrupe los elementos con la siguiente herramienta; ingrese al menú **Topology,** busque **Open Annotation Palette,** y aparecerá una ventana como se muestra en la figura 2.6, de nombre (**Annotation).**

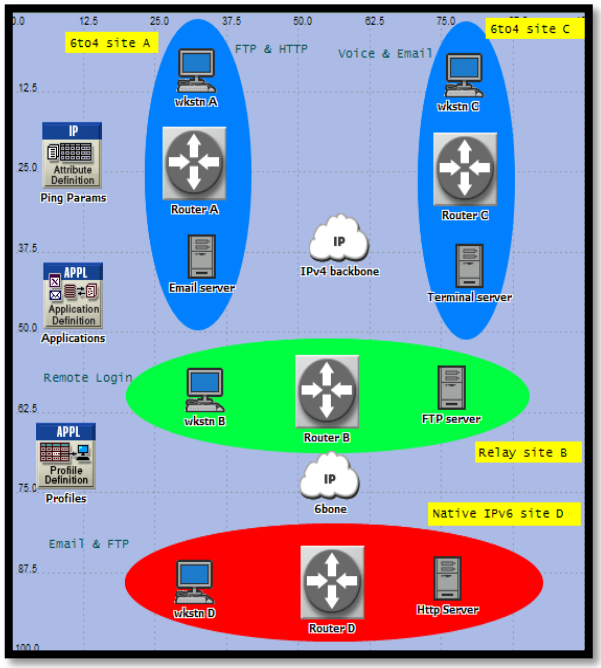
Figura 2.6. Annotation



Seleccione  y agrupe como se muestra a continuación, posteriormente oprima click derecho sobre cualquier borde del ovalo, e ingrese a **Edit Attributes,** en **fill,** que se encuentra con la opción **no fill,** actívela**,** para rellenar el ovalo. También puede cambiarle el color al ovalo, a su gusto. Para guardar cambios oprima en **OK.**

También coloque nombre a los grupos utilizando la herramienta  , al escoger esta opción sale una ventana **(Define Text Annotation),** edite el texto y cierre la ventana que automáticamente se guardara, ubíquese donde va a colocar el texto correspondiente. Puede cambiar de relleno utilice la opción **background color** y el color del texto como se hizo anteriormente. Quedara como se muestra en la figura 2.7.

Figura 2.7. Construcción de sitios 6to4



Una los diferentes elementos con enlaces de tipo **link model 100BaseT,** y **PPP_DS3** (estos se encuentran en el menú **object palette tree).** Conecté como se muestra en la tabla 2.4.

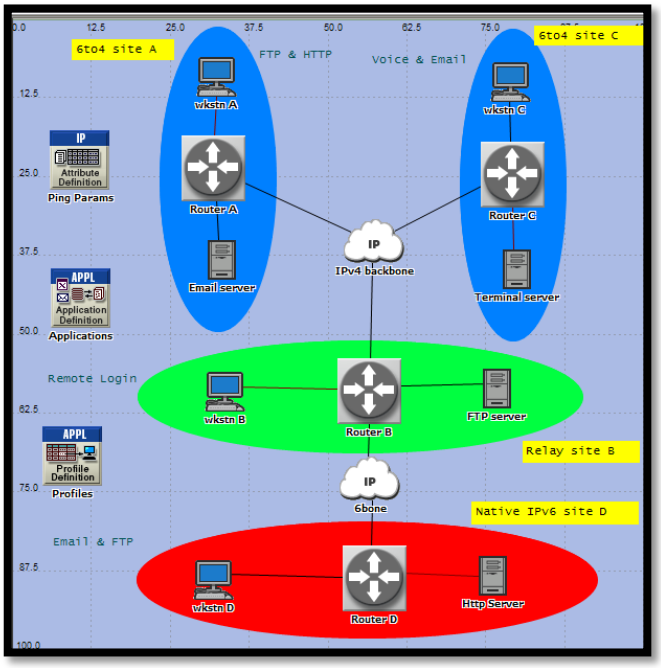
Tabla2.4. Conexiones de la red 6to4

Origen	Tipo de Enlace	Destino
Wkstn A	100BaseT	Router A
Wkstn C	PPP_DS3	Router C
Email Server	PPP_DS3	Router A
Router A	PPP_DS3	IPv4 backbone
Router C	100BaseT	Terminal Server
IPv4 backbone	PPP_DS3	Router C
Router B	PPP_DS3	IPv4 backbone
Wkstn B	100BaseT	Router B
FTP Server	PPP_DS3	Router B
Router B	PPP_DS3	6 bone
6 bone	PPP_DS3	Router D
Wkstn D	PPP_DS3	Router D
Router D	100BaseT	Http Server

Autores

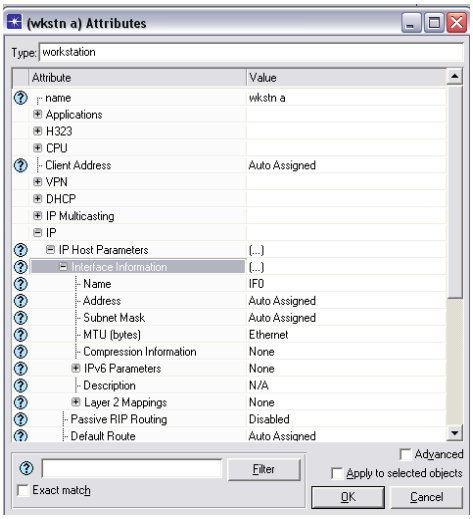
Quedando como se muestra en la figura 2.8.

Figura 2.8. Escenario 6to4 con Enlaces



Ubíquese en **wkstn A,** realice click derecho, seleccione **edit atrributes**; ahí encontrarà información de la estación. Los cambios que se harán son para indicar: dirección, submascara y el protocolo a utilizar; esto se hace desplegando la opción **IP** luego **IP Host Parameters,** posteriormente abra la opción **Interface Information** como se muestra en la siguiente figura 2.9.

Figura 2.9. Atributos de la red 6to4, wkstn A



En esta tabla se modifica:

- **Address,** oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne un nueva dirección IP por **192.0.6.1**
- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne 255.255.255.0.
- **MTU (bytes),** para esta estación debe estar en **Ethernet.**

Además en **IPv6 Parameters** oprimiendo click sobre el icono (+) se modificarà algunos parámetros:

- **Link Local Address** que se encuentra en la opción **Not Active ,** asigne **Default EUI-64**
- **Global Address (es)** despliegue el icono (+), y encontrara la opción **Not Active,** cambie **Address** que se está en **Not Active,** en **edit** por **2002:192.0.1.1:b::2**, y **Address Type** debe estar **Non EUI-64**
- **IP Host Parameters** en la opción **IPv6 Default Route** que se encuentra en **Auto Assigned,** se asigna la dirección **2002:192.0.1.1:b::1**, por último oprima **OK** para guardar los cambios realizados.

Este paso se repite para todas las **wkstn** pero cada una tiene asignado diferentes valores en los parámetros como se muestra en la tabla 2.5.

Forma rápida de configuración:

- **IP→ IP Host Parameters→ Interface Information:** Para cambiar Address y Subnet Mask
- **IP→ IP Host Parameters→ Interface Information→ IPv6 Parameters**: Para cambiar Link Local Address, Global Address (es) (Address, Address Type).
- **IP→ IP Host Parameters→ IPv6 Default Route.**

Tabla2.5. Configuración de los elementos de la red 6to4

	wkstn B	**wkstn C**	**wkstn D**
Address	192.0.12.2	192.0.3.1	192.0.8.2
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
MTU(bytes)	Ethernet	IP	IP
Link local address	Default EUI-64	Default EUI-64	Default EUI-64
Global address (es) **Address:** **Address Type:**	2003:1:1::2 Non EUI-64	2002:192.0.4.1:e::2 Non EUI-64	2003:2:2::2 Non EUI-64
IPv6 Default Route	2003:1:1::1	2002:192.0.4.1:e::1	2003:2:2::1

Autores

3.4 Visualización de la tabla de reportes: para visualizar la tabla de enrutamiento debe seleccionar cada **Router,** oprimir click derecho para seleccionar la opción **edit attributes**, buscar la opción **Reports,** desplegar **IP Forwarding Table** que se encuentra con **Do Not Export,** inmediatamente, busque la opción **Export at End Simulation,** y oprimir **OK.** Repita este procedimiento para los **Routers B, C, D.**

3.5 Configuración de los routers: ubíquese en el **Router A,** oprima click derecho y busque la opción **editt Attributes**, desplegué **IP,** luego en abra la opción **IP Routing Parameters,** sitúe **Interface Information (12rows)** y realice click en **(…)** aparecerá una tabla para editar direcciones **(Address)**, que se encuentran en **Auto Assigned,** busque **edit** para colocar la nueva dirección.
Como se muestra en la tabla 2.6. Forma rápida de configuración:

- **IP→ IP Routing Parameters→ Interface Information (12rows):** Para cambiar Address y Subnet Mask.

Tabla2.6. Configuración de los parámetros de orden físico y sub-interfaz del router A

	IF1	**IF10**	**IF11**
Address	192.0.6.2	192.0.2.2	192.0.1.1
Subnet Mask	255.255.255.0	255.255.255.0	Class C (natural)

Autores

Luego oprima click en **OK.**

Vuelva al menú de atributos, en IP despliegue la opción IP Routing Parameters, en la línea de **Loopback Interface** oprima click en **None,** y seleccione **edit,** aparece una ventana, en la parte inferior **(rows)** agregue una fila y realice los siguientes cambios en la tabla oprimiendo en la opción **edit** de cada casilla:

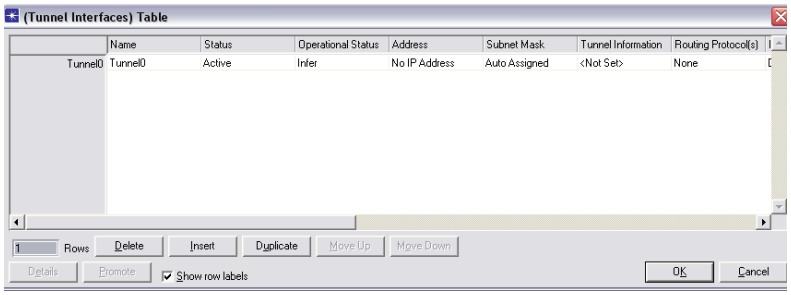
- Name: Loopback
- Address: 192.0.15.1
- Subnet mask: 255.255.255.0
- Routing protocol(s):**None**

Para finalizar oprima en la tabla **OK.**

Para la configuración el mecanismo de transición **6TO4_Manual** se realiza los siguientes pasos:

Despliegue el menú **IP,** busque **IP Routing Parameters,** donde se encuentra la opción **Tunnel Interfaces** que viene configurado con el valor **none;** haga click en **edit,** a continuación saldrá un ventana **(Tunnel Interfaces table).** En la parte inferior de la tabla **Tunnel Interface** se encuentra la opción **rows;** agregue una nueva fila colocando esta opción en 1. Quedando como se muestra en la figura 2.10.

Figura 2.10. Tunnel Interfaces



En la misma tabla en la opción **Tunnel Information,** que viene asignado con la opción **<Not Set>,** se debe oprimir y buscar **edit**, se abrirá una ventana **(Tunnel Information) Table,** donde asignara lo siguiente:

- Tunnel source: **IF11**
- Tunnel Mode: **IPv6 (6TO4)**
- Passenger protocol(s): **IPv4**

Finalice oprimiendo click en **OK** de la ventana de los **atributos** para que guarde los cambios realizados.

En la misma tabla de atributos del **Router A**, en la opción **IP**, seguido de **IPv6 Parameters**, despliegue **Static Routing Table,** donde aparece con el valor **None**, busque la opción **edit**, y saldrá una ventana **(Static Routing Table)**, en la parte inferior se debe agregar dos filas **(2 rows)** e inmediatamente se cambie los datos de la tabla 2.7.

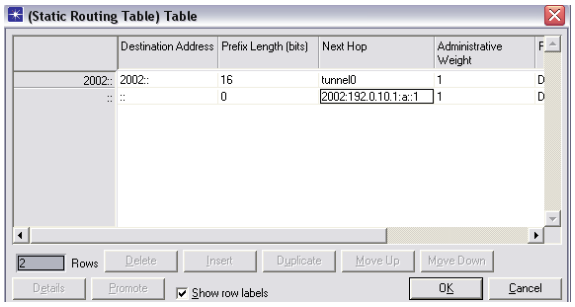
Tabla2.7. Configuración de las rutas estáticas de IPv6 en el router A

	Destination address	**Prefix length(bits)**	**Next hop**
1rows	2002::	16	tunnel0
2rows	::	0	2002:192.0.10.1:a::1

Autores

Quedando como se muestra en la figura 2.11.

Figura 2.11. Tunnel Interfaces IPv6



Oprima click en **OK,** para guardar cambios.

En la misma tabla de atributos, en la opción IP**,** seguido de IPv6 Parameters**,** se encuentra **Interface information,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** que se encuentra en cero (0), edite el número 2.

- Abra la opción **IF0**, coloque lo siguiente, **Link local address** en **Default EUI-64,** además despliegue el menú oprimiendo en el icono (+) de **Global Address (es)**, oprima click en **(…)**, busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit;** coloque **2002:192.0.1.1:c::1,** además **Address type** debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. En **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng.**

- Luego abra la otra opción **IF0**, donde se encuentra **Name** en **IF0**, busque **IF1** y colóquelo, automáticamente cambia el nombre. Posteriormente en la opción **Link local address** de estar en **Default EUI-64,** además en **Global Address (es)** oprima click en **None,** busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit,** coloque **2002:192.0.1.1:b::1,** además **Address type** debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. En **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng.**

Ahora bien, en la opción **IP,** seguido de **IPv6 Parameters,** se encuentra **Loopback Interfaces,** oprima click en **(+),** busque la opción **Number of Rows** y asigne **1,** posteriormente despliegue el menú de **Loopback ,** edite lo siguiente, **Link local address, Default EUI-64,** oprima click en **Global Address (es)** sobre

(…) examine la opción **edit,** donde aparece una ventana, la cual editara una fila **(1 Rows),** coloque los siguientes datos:

- **Address, 2002:192.0.1.1:d::1, y Address type, EUI-64**
  Para finalizar oprima en la tabla **OK,** y **Routing Protocol (s)** debe tener asignado el valor **RIPng.** Para guardar todos los cambios realizado oprima **OK.**

Seguimos en la tabla de atributos del **Router A** donde se crearà el último **Tunnel** que está en **IP**, seguido de **IPv6 Parameters**, en **Tunnel Interface** oprima click sobre **(…),** busque la opción **edit,** aparece una ventana **(Tunnel Interfaces Table),** agregue una fila **(1 Rows) y edite lo siguiente:**

- **Link local address, Default EUI-64,** oprima click en **Global Address (es)** sobre **None** examine la opción **edit,** donde aparece una ventana, la cual editarà una fila **(1 Rows),** coloque los siguientes datos, **Address** en **2002:192.0.1.1:a::1, Address type** en **Non EUI-64** y **Prefix Length(bits)** debe tener el valor de **128**. Para finalizar oprima click en **OK,** y **Routing Protocol (s)** debe estar deshabilitado **(None)**. Finalice oprimiendo click en **OK** sobre la tabla de atributos.

Para la configuración de los otros Routers, realice la siguiente configuración rápida y modifique los parámetros con la tabla 2.8.

ROUTER B

- **IP→ IP Routing Parameters→ Interface Information (12 Rows),** oprima click sobre (…), para cambiar Address y Subnet Mask.

Tabla2.8. Configuración de los parámetros de orden físico y sub-interfaz del router B

	IF1	IF4	IF10	IF11
Address	192.0.12.1	192.0.11.2	192.0.13.1	192.0.10.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0	Class C (natural)

Autores

Oprima en la tabla **OK.**

- **IP→ IP Routing Parameters → Loopback Interfaces,** oprima click sobre **(…)** y busque la opción **edit**, y agregue **1 Rows**, Para cambiar nombre, Address, Subnet Mask, Routing Protocol (s)
  - Name: loopback
  - Address: 192.0.19.1
  - Subnet Mask: 255.255.255
  - Routing protocol(s):None

  Para finalizar oprima en la tabla **OK.**

- **IP→ IP Routing Parameters →Tunnel Interfaces,** oprima click sobre **(…)** y busque la opción **edit** y agregue **1 rows,** en **Tunnel Information** oprima sobre **<Not Set>** y busque **edit,** cambie lo siguiente:
  - Tunnel Source: IF11
  - Tunnel Mode: IPv6 (6TO4)
  - Passenger Protocol(s): IPv4

  Para finalizar oprima en la tabla **OK**

- **IP→ IPv6 Parameters→Static Routing Table,** oprima click sobre **(…)** y busque la opción **edit,** teniendo en cuenta que solo será 1 fila nueva (1 Rows), digite la información de la tabla 2.9.

Tabla2.9. Configuración de las rutas estáticas de IPv6 en el router B

Destination address	Prefix length(bits)	Next hop
2002::	16	tunnel0

Autores

Para finalizar oprima en la tabla **OK.**

- **IP→ IPv6 Parameters→ Interface Information,** busque **edit,** tenga en cuenta que se agregan **3 Rows**, y asigne los valores que se encuentran en la tabla 2.10.

Tabla2.10. Configuración de los atributos de interfaces físicas de IPv6 del router B

Name	IF1	IF10	IF4
Link-local address	Default EUI-64	Default EUI-64	Default EUI-64
Global address(agregue 1 rows) **Address** **Address Type**	 2003:1:1::1 Non EUI-64	 2003:1:2::1 Non EUI-64	 2003:1:3::1 Non EUI-64
Routing Protocol	RIPng	RIPng	RIPng

Autores

Para finalizar oprima en la tabla **OK.**

- **IP→ IPv6 Parameters→ Loopback Interfaces**, oprima click sobre **(…)** y busque la opción **edit,** agregue **1 rows** y establezca los valores que se encuentran en la tabla 2.11.

Tabla2.11. Configuración de la interfaz de red virtual de IPv6 del router B

Name	Loopback
Link-local address	Default EUI-64
Global address(agregue 1 rows) **Address** **Prefix Length(bits)** **Address Type**	 2002:192.0.1.1:d::1 64 EUI-64
Routing Protocol	RIPng

Autores

Para finalizar oprima en la tabla **OK.**

- **IP→ IPv6 Parameters→ Tunnel Interfaces,** oprima click sobre **None** y busque la opción **edit,** agregue **1 rows** y establezca los valores que se encuentran en la tabla 2.12.

Tabla2.12. Configuración de los parámetros de los túneles de IPv6 del router B

Name	Tunnel0
Link-local address	Default EUI-64
Global address(agregue 1 rows) **Address** **Prefix Length(bits)** **Address Type**	 2002:192.0.10.1:a::1 128 Non EUI-64
Routing Protocol	None

Autores

Para finalizar oprima **OK** en la tabla de atributos, para finalizar con la configuración del Router B.

ROUTER C

- **IP→ IP Routing Parameters→ Interface Information (12 Rows),** oprima click sobre (…), para cambiar Address y Subnet Mask como se encuentra en la tabla 2.13.

Tabla2.13 Configuración de los parámetros de orden físico y sub-interfaz del router C

	IF1	**IF10**	**IF11**
Address	192.0.5.2	192.0.3.2	192.0.4.1
Subnet Mask	255.255.255.0	255.255.255.0	Class C(natural)

Autores

Oprima en la tabla **OK.**

- **IP→ IP Routing Parameters → Loopback Interfaces,** oprima click sobre **None** y busque la opción **edit**, y agregue **1 rows**, Para cambiar nombre, Address, Subnet Mask, Routing Protocol (s)
  - Name: loopback
  - Address: 192.0.14.1
  - Subnet Mask: 255.255.255
  - Routing protocol(s): None

  Oprima **OK,** para finalizar.

- **IP→ IP Routing Parameters →Tunnel Interfaces,** oprima click sobre **None** y busque la opción **edit,** agregue **1 rows,** y en **Tunnel Information** oprima sobre **<Not Set>** y busque **edit,** cambie lo siguiente:

  Tunnel source: IF11

  Tunnel mode: IPv6 (6TO4)

Passenger protocol(s): IPv4

Para finalizar oprima en la tabla **OK.**

- **IP→ IPv6 Parameters→Static Routing Table,** oprima click sobre **None** y busque la opción **edit,** teniendo en cuenta que se agregan 2 fila nueva (**2 rows**), digite los valores que se encuentran en la tabla 2.14.

Tabla2.14. Configuración de las rutas estáticas de IPv6 del router C

Destination address	**Prefix length(bits)**	**Next hop**
2002::	16	Tunnel0
::	0	2002:192.0.10.1:a::1

Autores

Para finalizar oprima en la tabla **OK.**

- **IP→ IPv6 Parameters→ Interface Information,** busque **None,** busque la opción **edit** tenga en cuenta que se agregan **2 rows**, y asigne los valores que se encuentran en la tabla 2.15.

Tabla2.15. Configuración de los atributos de interfaces físicas de IPv6 del router C

Name	IF10	IF1
Link-local address	Default EUI-64	Default EUI-64
Global address(agregue 1 rows) **Address** **Address Type**	2002:192.0.1.4:e::1 Non EUI-64	2002:192.0.4.1:f::1 Non EUI-64
Prefix Length (bits)	64	64
Routing Protocol	RIPng	RIPng

Autores

Nuevamente **OK** para realizar cambios

- **IP→ IPv6 Parameters→ Loopback Interfaces**, oprima click sobre **(…)** busque la opción **edit,** agregue **1 rows** y establezca los valores de la tabla 2.16.

Tabla2.16. Configuración de la interfaz de red virtual de IPv6 del router C

Name	loopback
Link-local address	default EUI-64
Global address(agregue 1 rows) **Address** **Address Type**	 2002:192.0.4.1:c::1 EUI-64
Prefix Length (bits)	64
Routing Protocol	RIPng

Autores

Para finalizar oprima en la tabla **OK.**

- **IP→ IPv6 Parameters→ Tunnel Interfaces,** oprima click sobre **None** y busque la opción **edit,** agregue **1 rows** y establezca los valores de la tabla 2.17.

Tabla2.17. Configuración de los parámetros de los túneles de IPv6 del router C

Name	Tunnel0
Link-local address	Default EUI-64
Global address(agregue 1 rows) **Address** **Address Type**	 2002:192.0.4.1:a::2 Non EUI-64
Prefix Length(bits)	128
Routing Protocol	None

Autores

Finalice oprimiendo **OK** sobre la tabla para guardar cambios.

Nuevamente haga click en **OK** en la tabla de atributos, para finalizar con la configuración de **Router C**.

ROUTER D

- **IP→ IP Routing Parameters→ Interface Information (12 Rows),** oprima click sobre (…), para cambiar Address y Subnet Mask; Como se muestra en la tabla 2.18.

Tabla2.18. Configuración de los parámetros de orden físico y sub-interfaz del router D

	IF0	**IF10**	**IF11**
Address	192.0.9.1	192.0.7.2	192.0.8.1
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0

Autores

Oprima en la tabla **OK.**

- **IP→ IP Routing Parameters→ Loopback Interfaces** oprima click sobre **None** y busque la opción **edit,** agregue **1 rows** y establezca los siguientes valores:

- Name: loopback
- Address: 192.0.18.1
- Subnet mask: 255.255.255.
- Routing protocol(s): None

Oprima **OK** en la tabla para guardar cambios.

- **IP→ IPv6 Parameters→Static Routing Table,** oprima click sobre **None** y busque la opción **edit,** teniendo en cuenta que se agregan una fila nueva (1row), digite los datos de la tabla 2.19.

Tabla2.19. Configuración de las rutas estáticas de IPv6 del router D

Destination Address	**Prefix length(bits)**	**Next hop**
2002::	16	2002:2:1::1

Autores

Oprima **OK** en la tabla para guardar cambios.

- **IP→ IPv6 Parameters→ Interface Information,** busque **None,** en la opción **edit** tenga en cuenta que se agregan **3 rows**, y asigne los valores de la tabla 2.20.

Tabla2.20. Configuración de los atributos de interfaces físicas de IPv6 del router D

Name	IF10	IF11	IF0
Link-local address	Default EUI-64	Default EUI-64	Default EUI-64
Global Address agregue 1 rows) **Address** **Address type**	 2003:2:1::1 Non EUI-64	 2003:2:2::1 Non EUI-64	 2003:2:3::1 Non EUI-64
Prefix Length (bits)	64	64	64
Routing Protocol(s)	RIPng	RIPng	RIPng

Autores

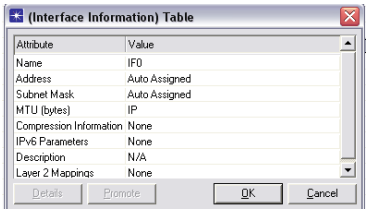
Oprima **OK** en la tabla para guardar cambios, nuevamente hágalo en la tabla de atributos, para finalizar con la configuración de Router D.

3.6 Configuración de los servicios: en el escenario que se tiene se deben configurar los siguientes servicios; **Email Server, Terminal Server, FTP Server y Http Server,** de la siguiente manera.

Ubíquese en **Email server,** realice click derecho, seleccione **Edit Atrributes**; ahí encontrara información de la estación. Los cambios que se harán son para indicar: dirección, submascara y el protocolo a utilizar.

Despliegue la opción **IP,** luego **IP Host Parameters,** posteriormente busque la opción **Interface Information** y realice click sobre (…), aparecerá una tabla como se muestra en la figura 2.12.

Figura 2.12. Interfaz de la Información de los servicios



Edite los siguientes parámetros:

- **Address,** oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne un nueva dirección IP por **192.0.2.1**
- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne **255.255.255.0**
- **MTU(bytes):** debe estar en **IP**

Finalice oprimiendo click sobre **OK.**

Además en **IP→IP Host Parameters →IP Interface Information→ IPv6 Parameters** oprimiendo click sobre el icono (+) se modificara algunos parámetros:

- **Link Local Address** en esta opción asigne **Default EUI-64**
- **Global Address (es)** despliegue el icono (+), y encontrara la opción **Not Active,** cambie **Address** que se está en **Not Active,** en **edit** por **2002:192.0.1.1:c::2**, y **Address Type** debe estar **Non EUI-64**

En **IP→IP Host Parameters** busque la opción **IPv6 Default Route** que se encuentra en **Auto Assigned,** asigne la dirección **2002:192.0.1.1:c::1**, por último oprima **OK** para guardar los cambios realizados.

Realice los pasos anteriores para la configuración de los otros servicios modificando algunos parámetros como se muestra en la tabla 2.21.

Tabla 2.21. Configuración de los servicios

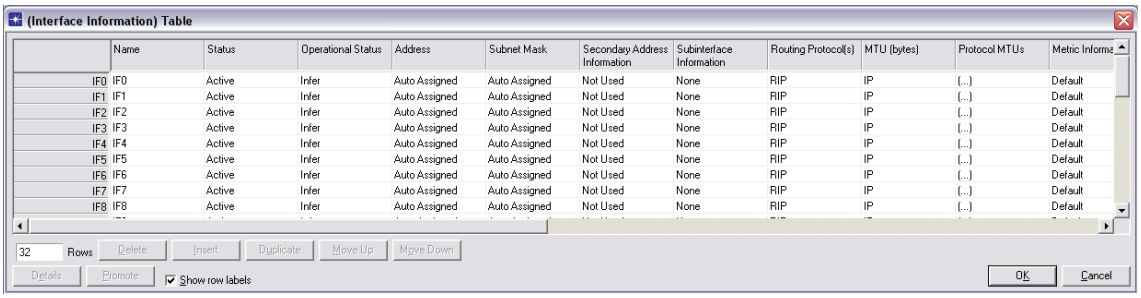
	Terminal server	FTP server	Http server
Address	192.0.5.1	192.0.13.2	192.0.9.2
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
MTU (bytes)	Ethernet	IP	IP
Link local address	Default EUI-64	Default EUI-64	Default EUI-64
Global Address (es) **Address:** **Address Type:**	 2002:192.0.4.1:f::2 Non EUI-64	 2002:1:2::2 Non EUI-64	 2003:2:3::2 Non EUI-64
IPv6 Default Route	2002:192.0.4.1:f::1	2003:1:2::1	2002:2:3::1

Autores

3.7 Configuración de las nubes: para la configuración de las nubes **IPv4 backbone** y **6bone** se realiza lo siguiente:

En la nube **IPv4 backbone,** realice click derecho, seleccione **Edit Atrributes**, busque **IP** luego **IP Routing Parameters,** posteriormente abra la opción **Interface Information (32rows)** y seleccione **(…)** y aparece una tabla como la que se muestra en la figura 2.13.

Figura 2.13. Interfaz de la Información de IPv4 backbone



Edite lo siguiente como se muestra en la tabla 2.22.

Tabla2.22. Configuración de los parámetros de orden físico y sub-interfaz de IPv4 backbone

	IF0	**IF1**	**IF2**
Address	192.0.1.2	192.0.4.2	192.0.10.2
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0

Autores

Oprima click en **OK** para guardar cambios.

Ahora en **IP→ IP Routing Parameters→ Loopback Interfaces,** oprima click en **None** y busque **edit,** aparece una ventana, y en la parte inferior **(rows)** agregue una fila **(1 rows)** y realice los siguientes cambios en la tabla oprimiendo en la opción **edit** de cada casilla:

- **Name:** loopback
- **Address:** 192.0.16.1
- **Subnet mask:** 255.255.255.0
- **Routing protocol(s):** None
- **MTU(bytes):** Ethernet

Para finalizar oprima en la tabla **OK.**

Se procede a configurar la **nube 6bone,** esto se realiza en los siguientes atributos:

Forma rápida de configuración:

- **IP → IP Routing Parameters →Interface Information (32rows)**, click sobre (…) y edite como se muestra en la tabla 2.23.

Tabla2.23. Configuración de los parámetros de orden físico y sub-interfaz de 6bone

	IF0	IF1
Address	192.0.11.1	192.0.7.1
Subnet Mask	255.255.255.0	255.255.255.0

Autores

Oprima click en **OK** para guardar cambios.

- **IP→ IP Routing Parameters→ Loopback Interfaces,** oprima click en **None** y busque **edit,** aparece una ventana, y en la parte inferior **(rows)** agregue una fila **(1 rows).** Coloque en las casillas lo siguiente
  - **Name:** loopback
  - **Address:** 192.0.17.1
  - **Subnet mask:** 255.255.255.0
  - **Routing protocol(s):** None
  - **MTU(bytes):** Ethernet

  Para finalizar oprima en la tabla **OK.**

- **IP→IPv6 Parameters→ Static Routing Table,** oprima click en **None**, busque **edit,** aparece una ventana, y en la parte inferior agregue una fila **(1 rows).** Coloque en las casillas lo siguiente:
  - **Destination Address:** 2002::
  - **Prefix Length (bits):** 16
  - **Next Hop:** 2003:1:3::1

  Para finalizar oprima en la tabla **OK**

- **IP→IPv6 Parameters→ Interface Information,** oprima click en **None**, busque **edit,** aparece una ventana, y en la parte inferior agregue dos filas **(2 rows).** Asigne los siguientes parámetros como se muestra en la tabla 2.24.

Tabla2.24. Configuración de los atributos de interfaces físicas de IPv6 de 6bone

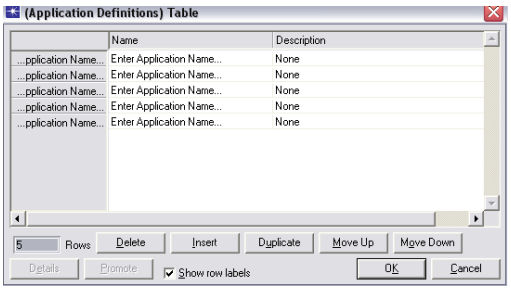
Name	**IF0**	**IF1**
Link-Local Address	Default EUI-64	Default EUI-64
Global Address(es) **Address** **Prefix Length(bits)** **Address Type**	 2003:1:3::2 64 Non EUI-64	 2003:2:1::2 64 Non EUI-64
Routing Protocol (s)	RIPng	RIPng

Autores

Oprima click en **OK** para guardar los cambios realizados y click en **OK** de la tabla principal de los Atributos.

3.8 Configuración de las aplicaciones: ahora se procede a configurar **Applications**, se oprime click sobre este modulo y seleccione **Edit Attributes**; busque la opción **Application Definitions,** oprima click sobre **(…)** seleccione **Edit,** posteriormente saldrá una ventana y en la parte inferior agregue **5 filas (rows),** como se muestra en la figura 2.14.

Figura 2.14. Definición de las aplicaciones



Edite lo siguientes parámetros como se muestra en la tabla 2.25.

Tabla2.25. Configuración de las aplicaciones

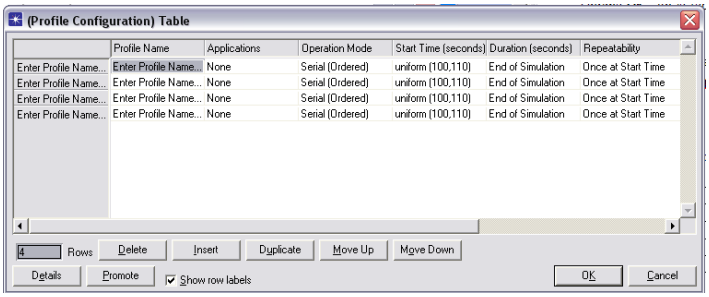
Name	Description
Web Application	Busque la opción **edit**, aparece una ventana y seleccione **Http** que tiene por defecto el valor **Off,** busque **Heavy Browsing.**
FTP Application	Busque la opción **edit**, aparece una ventana y seleccione **Ftp** que tiene por defecto el valor **Off,** busque **High Load.**
Remote login Application	Busque la opción **edit**, aparece una ventana y seleccione **Remote Login** que tiene por defecto el valor **Off,** busque **High Load**
Email Application	Busque la opción **edit**, aparece una ventana y seleccione **Email** que tiene por defecto el valor **Off,** busque **High Load**
Voice Application	Busque la opción **edit**, aparece una ventana y seleccione **Voice** que tiene por defecto el valor **Off,** busque **IP Telephony and Silence Suppressed.**

Autores

Oprima **OK** en la tabla**,** y en nuevamente **OK** en los atributos, para aplicar todos los cambios realizados.

3.9 Configuración de los perfiles: configure los **Profiles**, se oprime click sobre este icono y seleccione **Edit Attributes**; busque la opción **Profile Configuration,** oprima click sobre **None**, busque **edit,** aparece una tabla como la que se muestra en la figura 2.15 y agreguele **4 filas (rows).**

Figura 2.15. Configuración de los perfiles



Modifique el **Profile Name** por los nombres de la tabla 2.26.

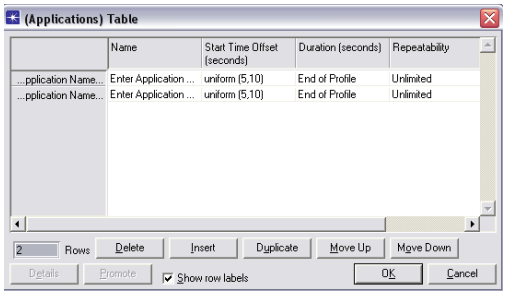
Tabla2.26. Nombre de los perfiles

Profile Name
FTP & Http
Voice & Email
Remote Login
Email & FTP

Autores

En la opción **Applications** de **FTP & Http,** que se encuentra en la tabla **(Profile Configuration Table)** y esta por defecto en el valor **None,** busque **edit**, aparece una tabla como se muestra en la figura 2.16 y agregue **2 filas (rows).**

Figura 2.16. Aplicaciones



Modifique las siguientes configuraciones como se muestra en la tabla 2.27.

Tabla2.27. Configuración de las aplicaciones FTP & Http

Name	Star Time Offset (Seconds)	Durations Seconds	Repeatability
Web Application	Uniform (5,10)	End to Profile	Once at star time
FTP Application	Uniform (5,10)	End to Profile	Once at star time

Autores

En **Applications Table,** oprima **OK** para guardar los cambios.

- En la opción **Applications** de **Voice & Email,** que se encuentra con el valor **None,** busque **edit**, aparece la tabla 2.28, agregue **2 rows**.

Tabla2.28. Configuración de las aplicaciones Voice & Email

Name	Star Time Offset (Seconds)	Durations Seconds	Repeatability
Voice Application	Uniform (5,10)	End to Profile	Once at star time
Email Application	Uniform (5,10)	End to Profile	Once at star time

Autores

En **Applications Table,** oprima **OK** para guardar los cambios.

- En la opción **Applications** de **Remote Login,** que se encuentra con el valor **None,** busque **edit**, aparece la tabla 2.29, y agregue **1 row**.

Tabla2.29. Configuración de la aplicacion Remote Login

Name	Star Time Offset (seconds)	Duration (seconds)	Repeatability
Remote login Application	Uniform (5,10)	End to profile	Unlimited

Autores

En **Applications Table,** oprima **OK** para guardar los cambios.

- En la opción **Applications** de **Email & FTP,** que se encuentra con el valor **None,** busque **edit**, aparece la tabla 2.30, y agregue **2 row.**

Tabla2.30. Configuración de las aplicaciones Email & FTP

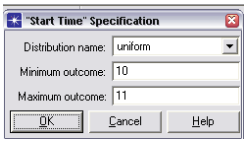
Name	Star Time Offset (Seconds)	Durations Seconds	Repeatability
Email Application	Uniform (5,10)	End to Profile	Once at star time
FTP Application	Uniform (5,10)	End to Profile	Once at star time

Autores

En **Applications Table,** oprima **OK** para guardar los cambios, seguidamente realice click en **OK,** en la tabla **(Profile Configuration table).**

Posteriormente despliegue el menú **Profile Configuration,** notarà que se han creado 4 aplicaciones, las cual se configuraran para ver el comportamiento de envió de paquetes. Abra el menú de; **FTP & Http,** busque la opción **Star Time (seconds)** que se encuentra con el valor de **uniform (100,110),** realice click sobre esta opción, aparece una ventana como la de la figura 2.17, donde debe cambiar **Mínimum outcome por 10** y **Máximum outcome por 11.** Realice este mismo procedimiento con; **Voice & Email, Remote Login y Email & FTP.**

Figura 2.17. Star Time



Seguidamente en el menú **Repeatability** que se encuentra en todas las aplicaciones debe estar en la opción **Unlimited.**

Realice click sobre **OK** en la ventana de **Profiles Attributes,** para efectuar cambios.

3.10 Habilitar Perfiles: ahora para habilitar las configuraciones que se hicieron en el punto pasado se realiza lo siguiente:

- Ubíquese en la **Wkstn A,** oprima click derecho, 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 como la de la tabla 2.31, agregue **1 Rows,** coloque lo siguiente:

Tabla2.31. Perfil admitido en la wkstn A

Profile Name	**Application Delay Tracking**
FTP & Http	Enabled

Autores

Oprima **OK,** en la tabla.

- Ahora seleccione la opción **Application: Supported Services,** y asigne el valor **All,** finalice oprimiendo click sobre **OK** en la tabla de atributos.

- En **Wkstn B,** oprima click derecho, 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 la información de la tabla 2.32.

Tabla2.32. Perfil admitido en la wkstn B

Profile Name	**Application Delay Tracking**
Remote Login	Enabled

Autores

Oprima **OK,** en la tabla.

- Ahora seleccione la opción **Application: Supported Services,** y asigne el valor **All,** finalice oprimiendo click sobre **OK** en la tabla de atributos.
- En **Wkstn C,** oprima click derecho, 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 la información de la tabla 2.33.

Tabla2.33. Perfil admitido en la wkstn B

Profile Name	**Application Delay Tracking**
Voice & Email	Enabled

Autores

Oprima **OK,** en la tabla.

- Ahora seleccione la opción **Application: Supported Services,** y asigne el valor **All,** finalice oprimiendo click sobre **OK** en la tabla de atributos.
- En **Wkstn D,** oprima click derecho, 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 la información de la tabla 2.34.

Tabla2.34. Perfil admitido en la wkstn B

Profile Name	Application Delay Tracking
Email & FTP	Enabled

Autores

Oprima **OK,** en la tabla.

- Ahora seleccione la opción **Application: Supported Services,** y asigne el valor **All,** finalice oprimiendo click sobre **OK** en la tabla de atributos.

3.11 Habilitador de soporte en cada servicio: ahora se habilita el soporte en cada **Server,** de la siguiente manera:

- En **Email Server** oprima click derecho y busque **Edit Attributes,** despliegue el menú **Applications,** seleccione **Application: Supported Services,** y habilite la opción **All.**
- Realice este mismo procedimiento con; **Terminal server, FTP Server y Http Server.**

3.12 Selección de resultados: En el escenario principal, realice click derecho, seleccione la opción **Choose individual DES statistics,** seleccione lo de la tabla 2.35.

Tabla 2.35. Selección de Resultados

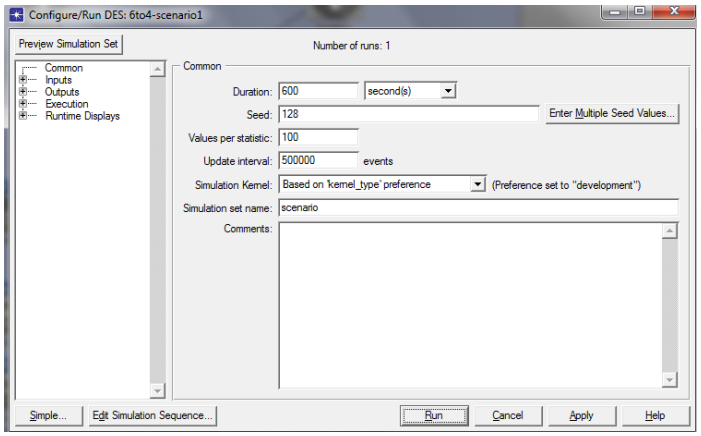
Link Statistics
• **point-to-point**
✓ throughput (bits/sec)- ->
✓ throughput (bits/sec) <- -

Autores

3.13 Realización de simulación: Para llevar a cabo la simulación, realice los siguientes pasos;

- En la barra de herramientas se encuentra el icono RUN  donde aparece una ventana mostrando la duración de la simulación; esta duración se puede modificar para ver mayores intervalos de tiempo. Asigne el siguiente; Duration 600 segundos, seed 128, values per statistics 100, Update interval 100000.como se muestra en la figura 2.18.

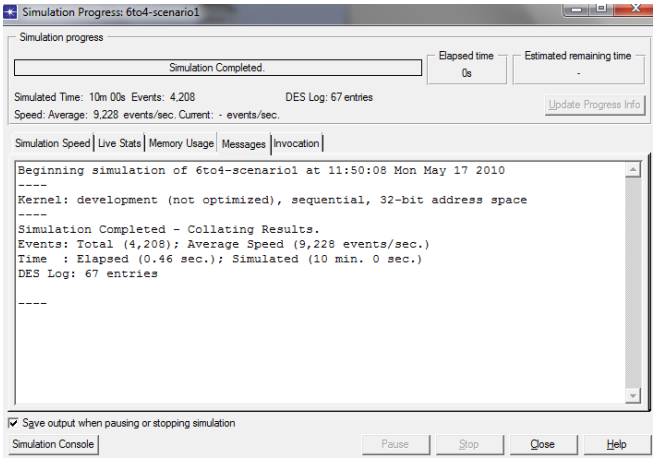
Figura 2.18. Parámetros de la simulación



Después de configurar este parámetro, haga click en **RUN**.

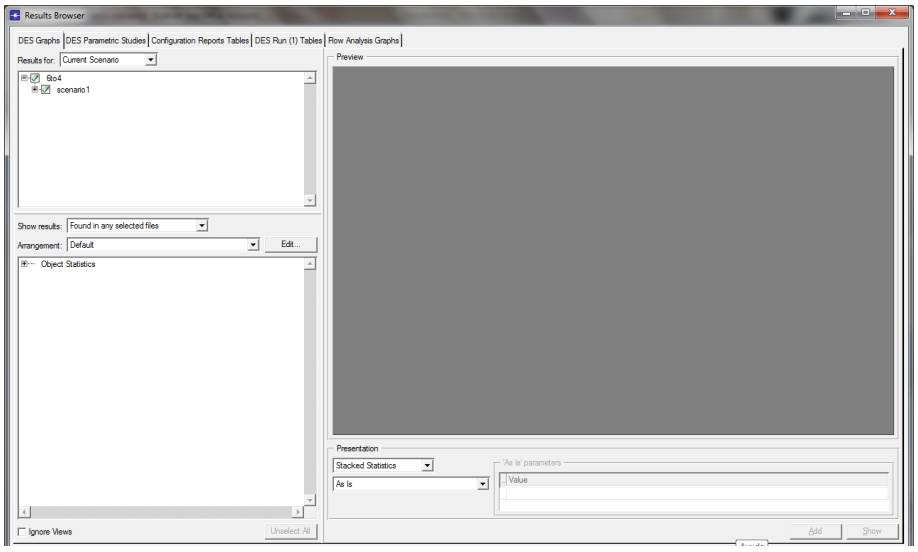
De esta manera al terminar el proceso de detección de errores se cierra la ventana en el botón **close** y aparece la figura 2.19.

Figura 2.19. Detector de Errores



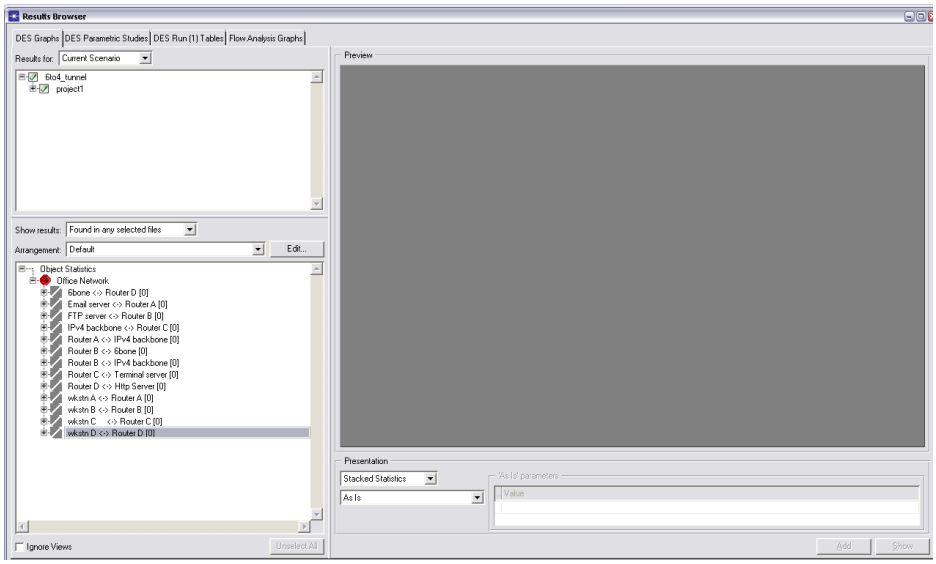
3.14 Resultados: Para revisar la tabla de resultados se ingresa al menú **Flow Analysis,** posteriormente se buscarà **Results**, se dará click en **View Results** y aparece la figura 2.20 (**Result Browser)**, donde se debe ingresar a la pestaña **DES Graphs.**

Figura 2.20. Resultados del Navegador



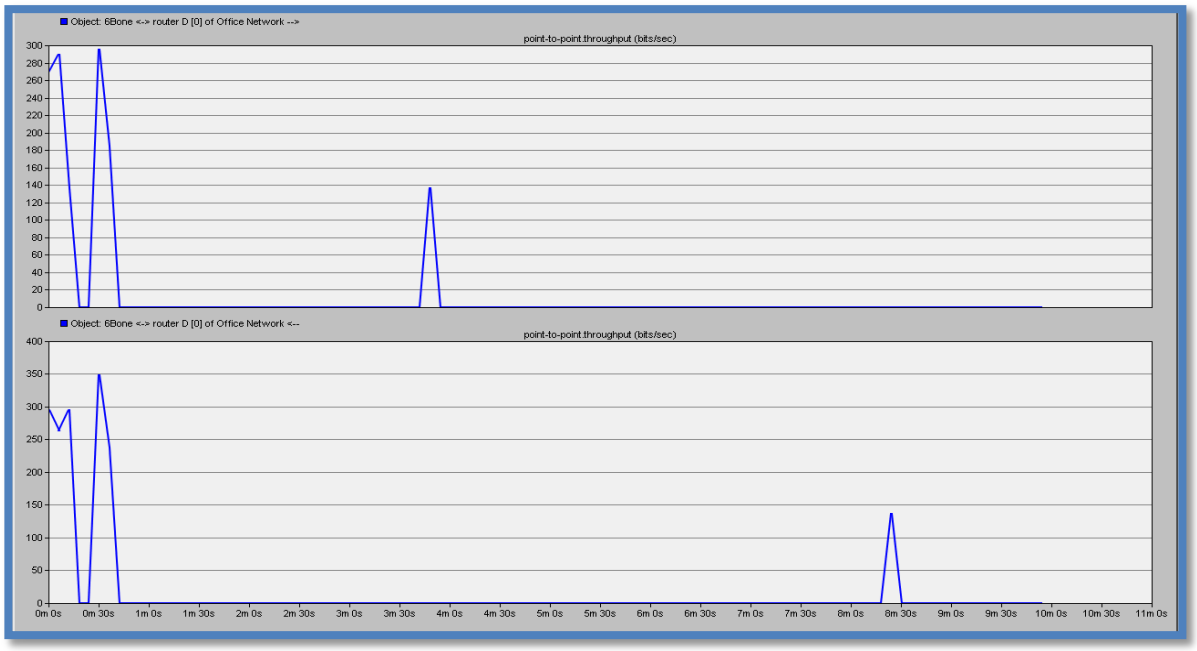
Para lograr observar el movimiento del tráfico y envió de paquetes (recibidos y enviado) que se encuentra en los 12 enlaces de cada uno de los elementos de la práctica; Ingrese a **Object Static** que se encuentra en la parte inferior de la ventana, y desplegue todo el menú para observar las gràficas como se muestra en la figura 2.21.

Figura 2.21. Visualización de Resultados

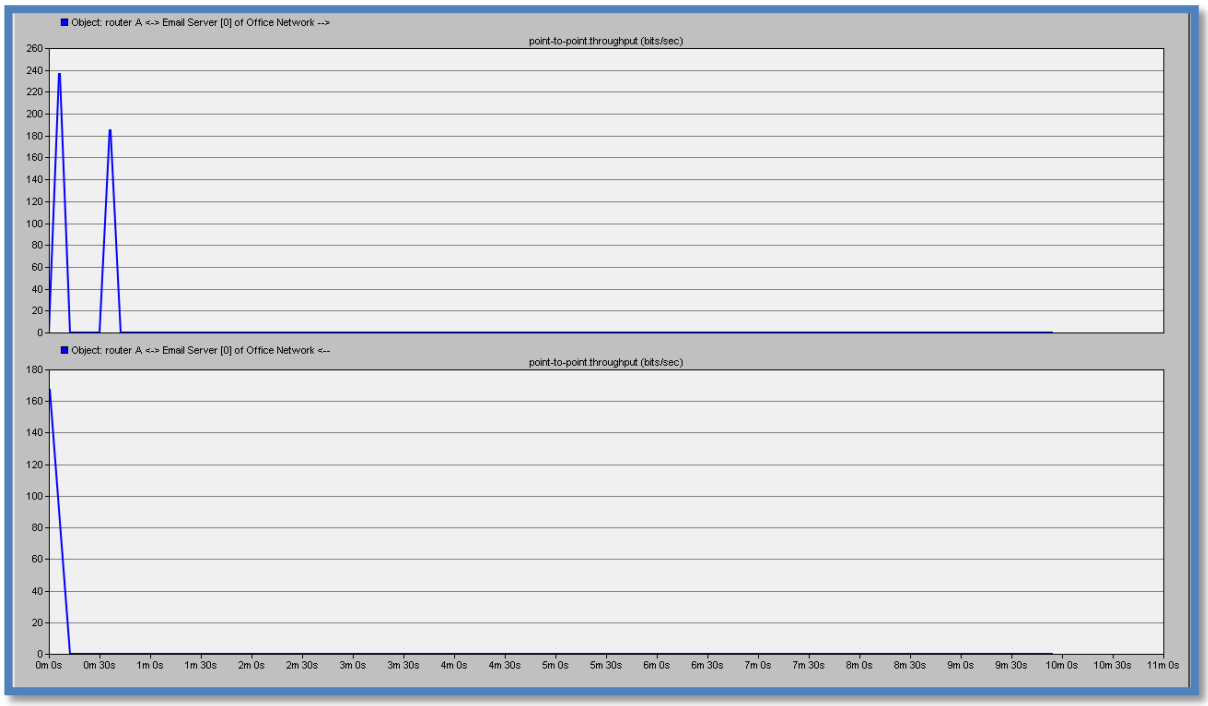


A continuación se encontraran posibles gráficos que representan el tráfico en bits/sec de cada enlace hecho en el escenario.

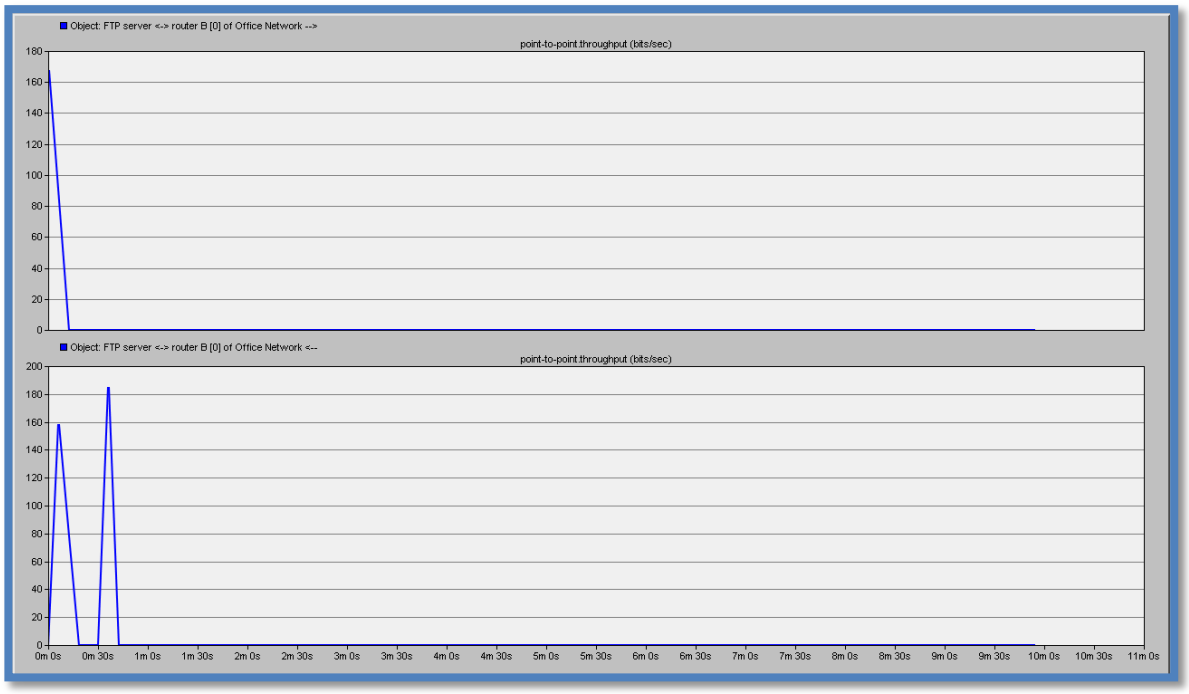
6bone <->Router D



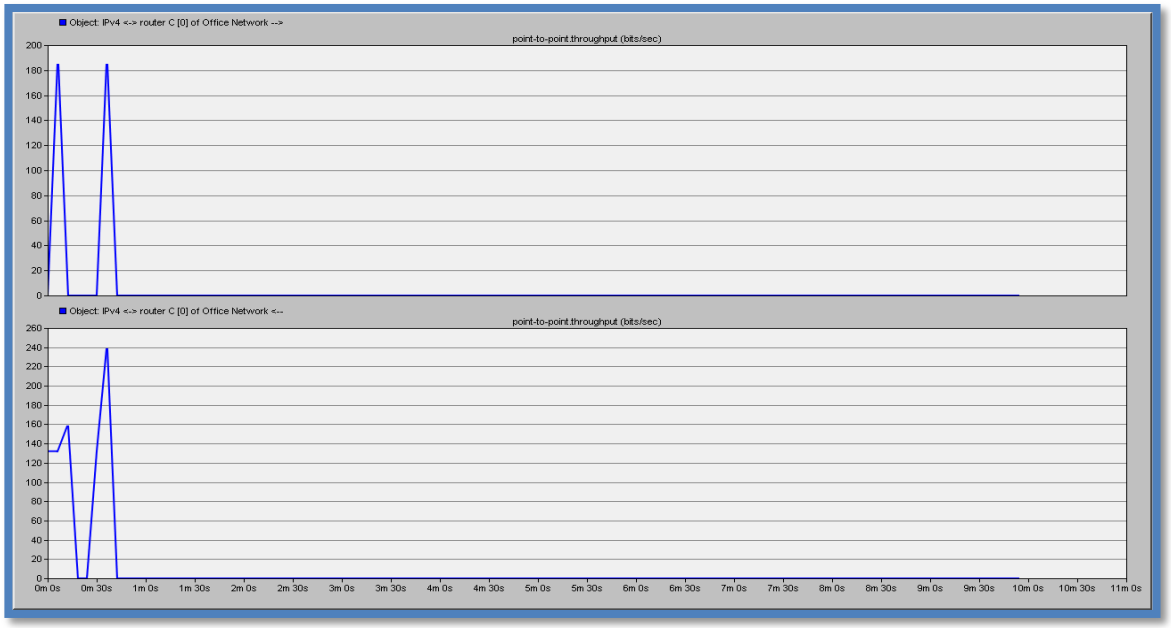
Router A <-> Email server



FTP server <-> Router B



IPv4 backbone <->Router C



En la misma figura 2.21, en la parte superior seleccione la pestaña **DES Run (1)** Tables, y despliegue la opción **Object Tables**, posteriormente abra todos los menú que hay, hasta encontrar la opción **Performance** , oprima click sobre **IP Forwarding Table at End of Simulation** y **IPv6 Forwarding Table at 600 seconds**, allí saldrán las figura 2.22 ,2.23, 2.24 y 2.25; estas son algunas de la tablas que se podrán encontrar como resultados.

Estas tablas contienen información de la ruta que realiza cada paquete que es enviado y recibido en el escenario, además se logran observar información importante como la fuente, siguiente salto y túneles configurado en la red.

ROUTER A

Figura 2.22. IP Forwarding Table at End of Simulation del router A

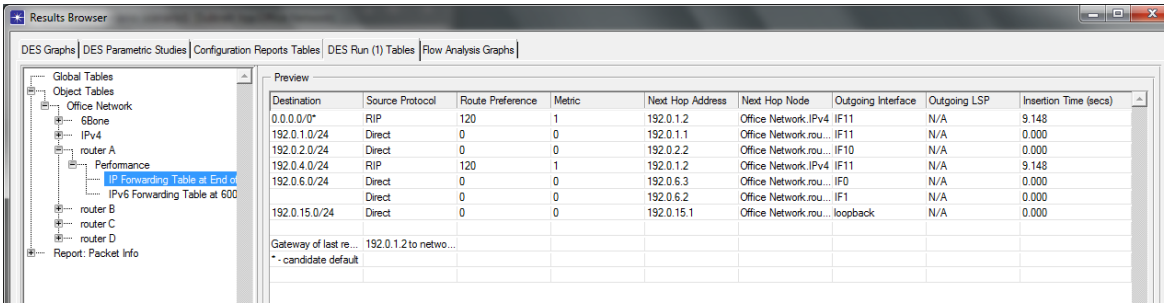
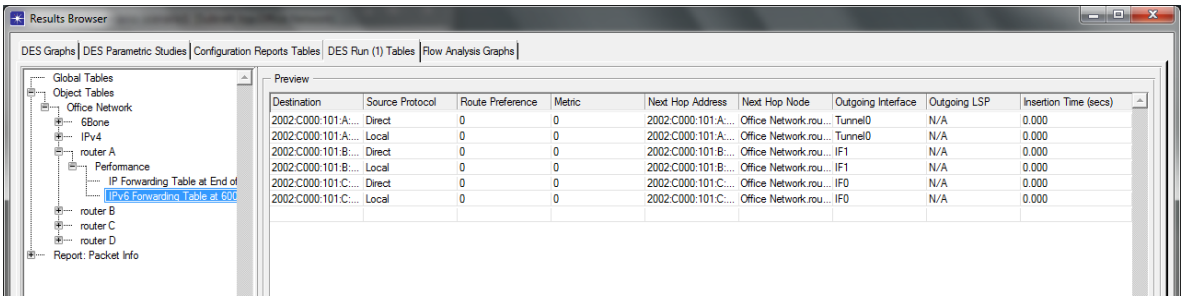


Figura 2.23. IPv6 Forwarding Table at 600 seconds del router A



ROUTER B

Figura 2.23. IP Forwarding Table at End of Simulation del router B

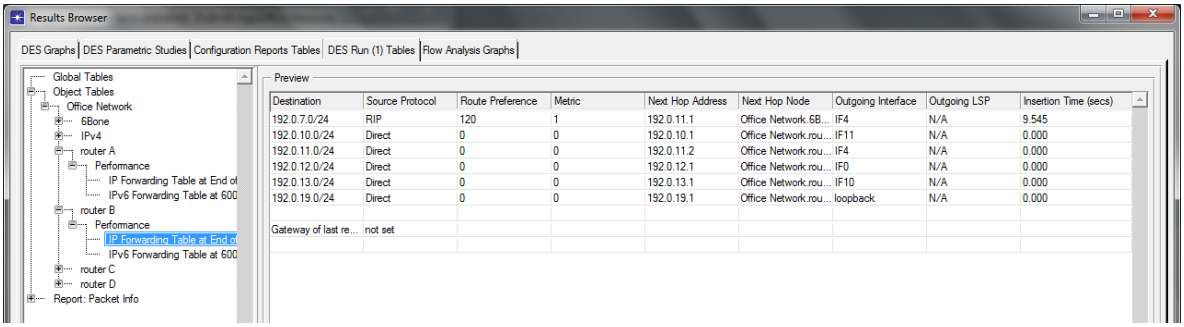
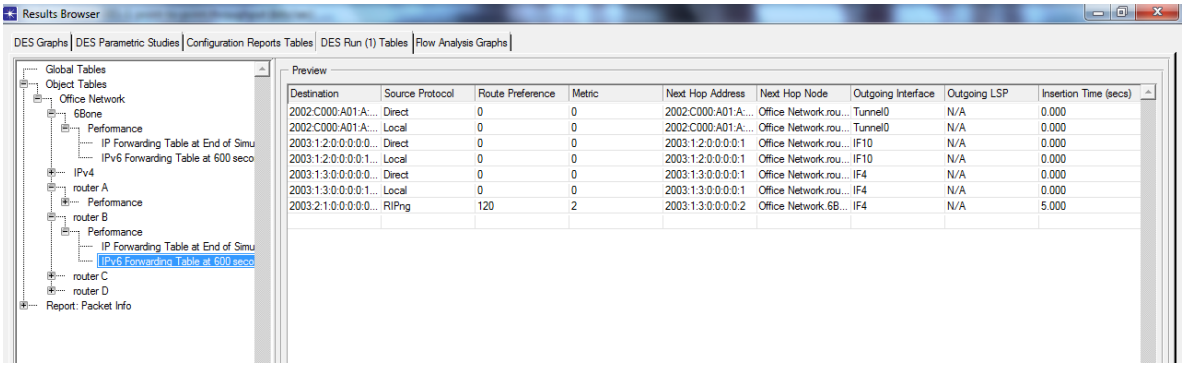


Figura 2.24. IPv6 Forwarding Table at 600 seconds del router B



Tareas:

- Comparar las tablas de enrutamiento de cada uno de los routers y analizar las diferencias que existen entre ellas.

- Comparar las tablas de enrutamiento de IPv6 para verificar la trayectoria que tiene el tráfico.

Practica N. 3

TITULO: MDRR_IPv6_IPv4

OBJETIVOS

- Analizar la calidad de servicio (QoS) en aplicaciones como transmisión de video o voz.
- Estudiar el mecanismo que realizan los routers para garantizar calidad del servicio en las redes IPv6, utilizando el algoritmo de planificación MDRR.

1. MARCO TEÓRICO

QoS: (Quality of Service) La calidad de servicio es primordial para cualquier red de convergencia de servicios. En general, QoS se refiere a la habilidad de suministrar un servicio adecuado a cada tipo de tráfico. Hoy en día existen dos tipos de tecnologías para el soporte de QoS, la Arquitectura de Servicios Integrados y la Arquitectura de Servicios Diferenciados.

ToS: (Type of Service) Los bits de tipo de servicio se incluyeron en la cabecera IPv4 para permitir diferenciar diversos tipos de datagramas IP (por ejemplo, datagramas que requieran un bajo retardo, altas prestaciones, o una fiabilidad especial). Por ejemplo, sería útil distinguir los datagramas de servicios de tiempo real (por ejemplo, para una aplicación de telefonía IP) de los datagramas de servicios elásticos (como FTP). Estos bits se utilizan para identificar el tipo de tratamiento que se le deben dar a los paquetes en las colas que ingresan a un router. [25]

[25] REDES DE COMPUTADORES un enfoque descendente Basado en Internet, 2da edición. 2004. PEARSON Addison Wesley

ACL: (Access Control List) En un router las listas de control de acceso permiten el ingreso de los paquetes al router de acuerdo con ciertas reglas de identificación (ejemplo paquetes que tienen cierta dirección IP de origen)

DRR: (Deficit Round Robin) Permite así enviar paquetes de longitud variable con un mejor desempeño. Funciona en dos variables, una llamada *quantum* que indica la cantidad de bits a enviar en cada turno de transmisión y otra llamada contador de déficit (*déficit counter)* que se encarga de almacenar el valor del *quantum* obtenido al transmitir un paquete y que permitirá posteriormente enviar paquetes de longitud variable.[26]

MDRR: Una variación de la DRR que se enfoca en la minimización del retardo para un ciertos flujos de tráfico. Esto es útil, por ejemplo, en el manejo de paquetes de VoIP. Aunque los flujos VoIP necesitan tanto garantías de ancho de banda, como garantías de retardo de los paquetes, podemos pensar en un acercamiento alternativo de proporcionar una garantía de ancho de banda con retrasos mínimos (minimizar la demora). El esquema MDRR se centra en la forma de minimizar los retrasos o demoras con base en el esquema de planificación DRR. por ejemplo, puede hacerse una modificación asignando prioridades a las colas de espera, lo que sirve como una planificación de prioridades para diferentes colas. por ejemplo, se podría definir una cola con ultra alta prioridad, la cual siempre obtendrá prioridad si tiene paquetes para enviar y no se le limitara el tamaño del Quantum. La palabra "modificación" en MDRR no necesariamente tiene esta aproximación; se pueden hacer diferentes modificaciones. Vale la pena

[26] Algoritmos de planificación en redes de paquetes, Juan Carlos Cuellar Quiñonez. http://bibliotecadigital.icesi.edu.co/biblioteca_digital/bitstream/item/2135/1/algoritmos_planificacion.pdf.

señalar que la mayoría de los vendedores de routers en la actualidad implementan alguna forma de cola de espera MDRR.[27]

TABLA DE COMPARACIÓN: esta tabla indica la comparación entre el nivel de prioridad que asigna el software Opnet y DSCP

Tabla3.1. Taba de prioridad

OPNET	**DSCP(*Differentiated Services Code Point*)**
Best Effort (0)	BE Best Effort
Background (1)	AF1 Assured Forwarding
Standard (2)	AF2 Assured Forwarding
Excellent Effort(3)	AF2 Assured Forwarding
Streaming Multimedia(4)	AF3 Assured Forwarding
Interative Voice (6)	EF Expedited Forwarding

Autores

2. DESCRIPCIÓN DEL ESCENARIO

La red presenta una situación de cuello de botella. La red se compone de cuatro clientes y cuatro servidores, cada par usa un ToS diferente para la transferencia de datos. El switch A y B, hacen la función de capa de acceso. El trafico generado por cada nodo cliente es de aproximadamente 600.000 bps. Los nodos 1 y 3 generan trafico IPv4 mientras que los nodos 2 y 4 generan trafico IPv6. Los sistemas finales (cliente-servidor) poseen diferentes aplicaciones (tales como; Email, File Transfer, Video Conferencing, etc.) El algoritmo de planificación que

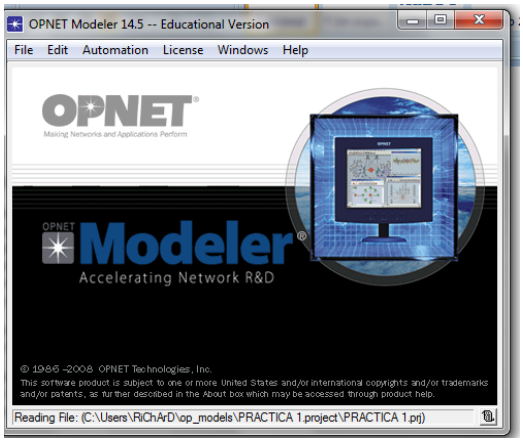
[27] Network Routing. Algorithms, Protocols, and Architectures. DEEPANKAR MEDHI, KARTHIKEYAN RAMASAMY.

se utiliza para que los routers ofrezcan calidad de servicio es el MDRR. Las clases de tráfico se utilizan en esta práctica para clasificar los paquetes y brindar soporte de QoS, según las políticas de tráfico.

3. PASOS A SEGUIR

Ejecutar el programa como se muestra en la figura 3.1.

Figura 3.1. Interfaz de OPNET



3.1 Creación de un nuevo proyecto: Vaya a la opción **File** de la barra de herramientas y selecciones la opción **New**. A continuación aparecerá una ventana donde se solicita el tipo de proyecto. Seleccione la opción **Project** y luego haga click en **OK**. (**Descripción rápida:** File→ New→ Project → ok).

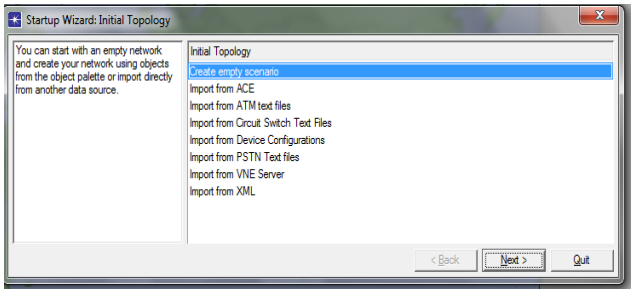
Project name → <MDRR_IPv6_IPv4>

Scenario name→ project 1→ok.

Asegúrese de que se encuentre seleccionada la opción **starup wizard.**

3.2 Configuración del escenario de la red: a continuación aparecerá la figura 3.2, que muestra la ventana inicial del ayudante. Seleccione: (Startup wizard: initial topology → create empty scenario→ next).

Figura 3.2.Startup wizard initial topology

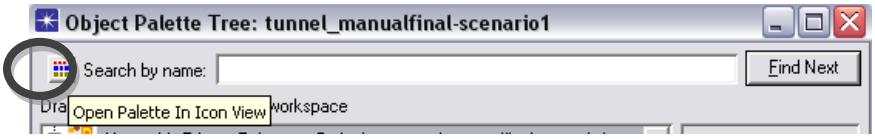


A continuación aparece la opción de selección de la escala de la red. Seleccione: (Logical→ next).

Ahora aparece el menú de tecnologías disponibles; seleccione las tecnologias **Internet_toolbox, Ethernet_advanced, routers_advanced y links_advanced**: (select Technologies→ Internet_toolbox, Ethernet advanced, routers_advanced, links_advanced →next→Finish).

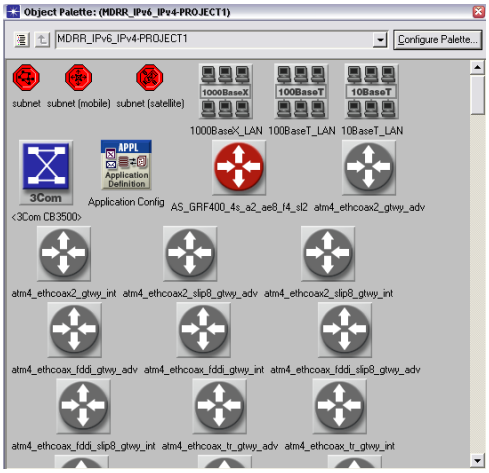
3.3 Creación de la red: Aparece un espacio de trabajo de color gris en el cual se creara la topología; Diríjase a la barra de herramientas y haga click en el icono  **Object Palette Tree** como se muestra en la figura 3.3; seleccione **Open Palette In Icon View**

Figura 3.3. Object Palette Tree



Allí se desplegaran los iconos como se muestra en la figura 3.4, de los diferentes dispositivos de las tecnologías.

Figura 3.4. Elementos de la red



Ahora agregue los elementos que se encuentran en la tabla 3.2.

Tabla3.2. Elementos de la red MDRR IPv6-IPv4

Cantidad	Módulos
8	ethernet_wkstn_adv
2	ethernet8_switch_adv
2	ethernet2_slip8_gtwy_adv
1	Application Config
1	Profile Config
1	QoS Attribute Config

Autores

A continuación edite los nombres de cada dispositivo como se encuentra en la tabla 3.3; oprimiendo click derecho sobre cada icono y seleccionando la opción **Set name**.

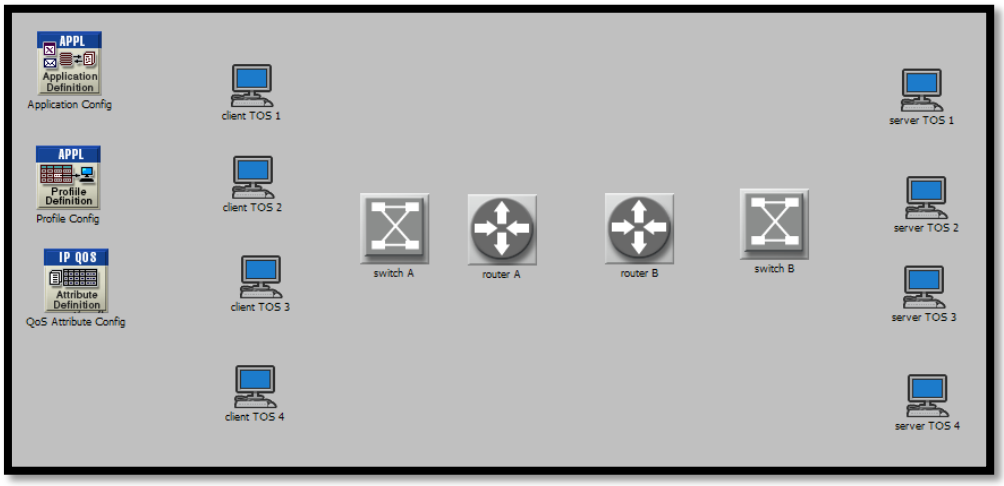
Organice los elementos de la red como se encuentra en la figura 3.5.

Tabla3.3. Nombres de los elementos de la red MDRR IPv6-IPv4

Modelo	Nombre
ethernet_wkstn_adv	client TOS 1
ethernet_wkstn_adv	client TOS 2
ethernet_wkstn_adv	client TOS 3
ethernet_wkstn_adv	client TOS 4
ethernet_wkstn_adv	server TOS 1
ethernet_wkstn_adv	server TOS 2
ethernet_wkstn_adv	server TOS 3
ethernet_wkstn_adv	server TOS 4
ethernet8_switch_adv	switch A
ethernet8_switch_adv	switch B
ethernet2_slip8_gtwy_adv	router A
ethernet2_slip8_gtwy_adv	router B
Application Definition	Application Config
Profile Definition	Profile Config
Attribute Definition	QoS Attribute Config

Autores

Figura 3.5. Escenario Qos



Una los diferentes elementos con enlaces de tipo **link model 10BaseT_int, 10BaseT y ppp_adv** (estos se encuentran en el menú **object palette tree).** Conectélos como se encuentra en la tabla 3.4.

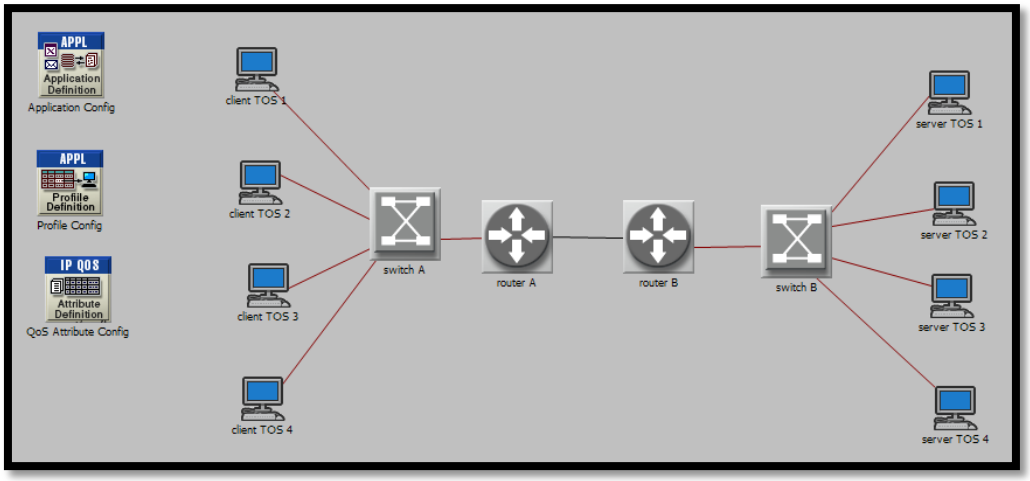
Tabla 3.4. Conexiones de la red MDRR IPv6-IPv4

Origen	TIPO DE ENLACE	Destino
client TOS 1	**10BaseT_int**	switch A
client TOS 2		
client TOS 3		
client TOS 4		
Switch A	**10BaseT**	router A
Router A	**ppp_adv (⟷)**	router B
Router B	**10BaseT**	switch B
Switch B	**10BaseT**	server TOS 1
		server TOS 2
		server TOS 3
		server TOS 4

Autores

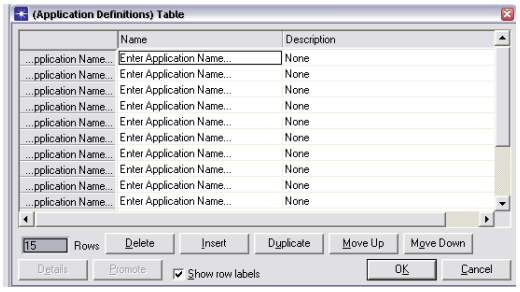
Quedando la red como se encuentra en la figura 3.6.

Figura 3.6. Escenario 6to4 con los enlaces



3.4 Configuración de las aplicaciones: Ahora se procede a configurar el modulo **Applications Config**. Para ello, oprima click sobre este icono, seleccione **Edit Attributes**; busque la opción **Application Definitions,** oprima click sobre **None,** seleccione **Edit,** posteriormente saldrá la figura 3.7 y en la parte inferior agregue **15 filas (rows).**

Figura 3.7. Definición de las aplicaciones



A continuación en cada fila cree las siguientes aplicaciones:

- **Database Access (Heavy):** Busque la opción **edit** de la columna **Description**, aparece una ventana y seleccione **Database** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.5 que deberá quedar con las siguientes especificaciones:

Tabla3.5. Configuración Database

Transaction Mix (Queries/Total Transactions)	50%
Transaction Interarrival Time(seconds)	**Distribution name:** exponential **Mean outcome:** 12
Transaction Size(bytes)	**Distribution name:** Constant **Mean outcome:** 32768
Symbolic Server Name	Database Servert
Type of Service	Best Effort (0)
RSVP Parameter	None
Back- End Custom Application	Not used

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Database Access (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Datebase** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.6 que deberá quedar con las siguientes especificaciones:

Tabla3.6. Configuración Database Access (Light):

Transaction Mix (Queries/Total Transactions)	50%
Transaction Interarrival Time(seconds)	**Distribution name:** exponential **Mean outcome:** 30
Transaction Size(bytes)	**Distribution name:** constant **Mean outcome:** 16
Symbolic Server Name	Database Servert
Type of Service	Best Effort (0)
RSVP Parameter	None
Back- End Custom Application	Not used

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Email (Heavy):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Email** que tiene por defecto el valor **Off,** busque **High Load** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios.
- **Email (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Email** que tiene por defecto el valor **Off,** busque **low load** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **File Transfer (Heavy):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Ftp** que tiene por defecto el valor **Off.**

Elija nuevamente **edit,** y aparecerá una tabla 3.7 que deberá quedar con las siguientes especificaciones:

Tabla3.7. Configuración File Transfer (Heavy)

Command Mix (Get/total)	**50%**
Inte-Request Time(Seconds)	**Distribution name:** Exponential **Mean outcome:** 360
File Size(bytes)	**Distribution name:** Constant **Mean outcome:** 50000
Symbolic Server Name	**FTP Server**
Type of service	**Best Effort (0)**
RSVP Parameter	**None**
Back- End Custom Application	**Not used**

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **File Transfer (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Ftp** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.8 que deberá quedar con las siguientes especificaciones:

Tabla 3.8.Configuración File Transfer (Light)

Command Mix (Get/total)	50%
Inte-Request Time(Seconds)	**Distribution name:** Exponential **Mean outcome:** 3600
File Size(bytes)	**Distribution name:** Constant **Mean outcome:** 1000
Symbolic Server Name	FTP Server
Type of service	Best Effort (0)
RSVP Parameter	None
Back- End Custom Application	Not used

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **File Print (Heavy):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Print** que tiene por defecto el valor **Off,** busque **Color Prints** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **File Print (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Print** que tiene por defecto el valor **Off,** busque **Text File** y asigne este valor. Finalice oprimiendo **OK,** para realizar cambios**.**
- **Telnet Session (Heavy):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Remote Login** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.9 que deberá quedar con las siguientes especificaciones:

Tabla3.9.Configuración File Print (Heavy)

Inter Command Time-(Seconds)	**Distribution name:** Normal **Mean outcome:** 30 **Variance:** 5
Termial Traffic (bytes per command)	**Distribution name: Normal** **Mean outcome :** 60 **Variance:** 144
Host Traffic (bytes per command)	**Distribution name : Normal** **Mean outcome :** 25 **Variance:** 25
Symbolic Server Name	**Remote Login Server**
Type of service	**Best Effort (0)**
RSVP Parameter	**None**
Back- End Custom Application	**Not used**

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Telnet Session (Light):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Remote Login** que tiene por defecto el valor **Off,** busque **Low Load** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**

- **Video Conferencing (Heavy):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing** que tiene por defecto el valor **Off,** busque **VCR Quality Video** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **Video Conferencing (streaming Multimedia):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.10 que deberá quedar con las siguientes especificaciones:

Tabla3.10.Configuración Video Conferencing (streaming Multimedia)

Frame Interrival Time Information	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Interrival Time (seconds):** **Distribution name**: costant **Mean outcome:** 0.333 **Outcoming Stream Interrival Time (seconds):** **Distribution name**: constant **Mean outcome:** 0.333
Frame Size Information(bytes)	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500 **Outcoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500
Symbolic Destination Name	**Video Destination**
Type of service	**Streaming Multimedia(4)**
RSVP Parameter	**None**
Traffic Mix (%)	**All Discrete.**

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Video Conferencing (excellent effort):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.11 que deberá quedar con las siguientes especificaciones

Tabla3.11. Configuración Video Conferencing (excellent effort)

Frame Interrival Time Information	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Interrival Time (seconds):** **Distribution name:** constant **Mean outcome:** 0.333 **Outcoming Stream Interrival Time (seconds) :** **Distribution name:** constant **Mean outcome:** 0.0333
Frame Size Information (bytes)	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500 **Outcoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500
Symbolic Destination Name	**Video Destination**
Type of service	**Excellent Effort(3)**
RSVP Parameter	**None**
Traffic Mix (%)	**All Discrete.**

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Video Conferencing (Standart):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.12 que deberá quedar con las siguientes especificaciones.

Tabla3.12. Configuración Video Conferencing (standart)

Frame Interrival Time Information	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Interrival Time (seconds):** **Distribution name:** constant **Mean outcome:** 0.333 **Outcoming Stream Interrival Time (seconds) :** **Distribution name:** constant **Mean outcome:** 0.0333
Frame Size Information(bytes)	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500 **Outcoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500
Symbolic Destination Name	**Video Destination**
Type of service	**Standart (2)**
RSVP Parameter	**None**
Traffic Mix (%)	**All Discrete.**

Autores

- **Video Conferencing (background):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.13 que deberá quedar con las siguientes especificaciones:

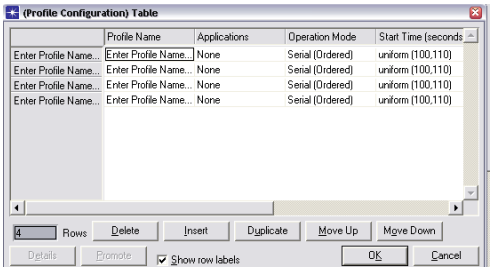
Tabla 3.13.Configuracion Video Conferencig (background)

Frame Interrival Time Information	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Interrival Time (seconds):** **Distribution name:** constant **Mean outcome:** 0.333 **Outcoming Stream Interrival Time (seconds) :** **Distribution name:** constant **Mean outcome:** 0.0333
Frame Size Information(bytes)	Busque la opción **edit**, aparece una tabla con dos parámetros: **Incoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500 **Outcoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 2500
Symbolic Destination Name	**Video Destination**
Type of service	**Background(1)**
RSVP Parameter	**None**
Traffic Mix (%)	**All Discrete.**

Autores

3.5 Configuración de los perfiles: Configure el **Profile Config**, haga click sobre este icono y seleccione **Edit Attributes**; busque la opción **Profile Configuration,** oprima click sobre **None**, busque **edit,** aparece la figura 3.8 y agreguele **4 filas (rows)**.

Figura 3.8. Configuración de los perfiles



A las filas modifique los campos de **Profile Name, Operation Mode y Star Time(seconds)** como se encuentra en la tabla 3.14.

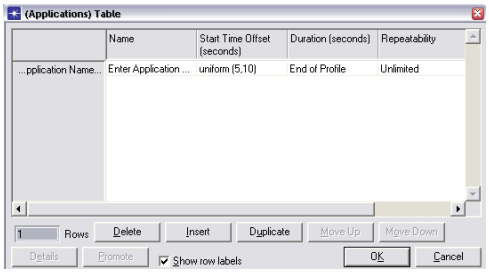
Tabla3.14 Configuración de Perfiles de Tráfico

Profile Name	**Operation Mode**	**Star Time (seconds)**
Background Traffic	Simultaneous	**Distribution Name:** constant **Mean outcome:** 100
Standard Traffic	Simultaneous	**Distribution Name:** constant **Mean outcome:** 100
Excellent Effort Traffic	Simultaneous	**Distribution Name:** constant **Mean outcome:** 100
Streaming Traffic	Simultaneous	**Distribution Name:** constant **Mean outcome:** 100

Autores

Además en la opción **Applications** de **Background Traffic,** que se encuentra en **(Profile Configuration Table)** y esta por defecto en el valor **None,** busque **edit**, aparecerá la figura 3.9 y agregue **1 fila (rows).**

Figura 3.9. Configuración del perfil Background Traffic



Modifique los parámetros que se encuentran en la tabla 3.15.

Tabla3.15 .Configuración de Background Traffic

Name	**Star Time Offset (Seconds)**	**Durations Seconds**	**Repeatability**
Video Conferencing (background)	**Distribution Name:** constant **Mean outcome:** 10	End to Profile	Once at star time

Autores

En **Applications Table,** oprima **OK** para realizar los cambios.

- En la opción **Applications** de **Standard Traffic,** que se encuentra en **(Profile Configuration Table)** y esta por defecto en el valor **None,** busque **edit**, aparecerá la tabla 3.16, y agregue **1 fila (rows)**

  Modifique lo siguiente en la tabla:

Tabla3.16. Configuración de Standard Traffic

Name	**Star Time Offset (Seconds)**	**Durations Seconds**	**Repeatability**
Video Conferencing (Standard)	**Distribution Name:** constant **Mean outcome:** 10	End to Profile	Once at star time

Autores

- En la opción **Applications** de **Excellent Effort Traffic,** que se encuentra en **(Profile Configuration Table)** y esta por defecto en el valor **None,** busque **edit**, aparecerá la tabla 3.17, y agregue **1 fila (rows)**

Tabla 3.17. Configuración de de Excellent Effort Traffic

Name	Star Time Offset (Seconds)	Durations Seconds	Repeatability
Video Conferencing (Excellent Effort)	**Distribution Name:** constant **Mean outcome:** 10	End to Profile	Once at star time

Autores

- En la opción **Applications** de **Streaming Traffic,** que se encuentra en **(Profile Configuration Table)** y esta por defecto en el valor **None,** busque **Edit,** aparecerá una tabla, y agregue **1 filas (rows)**.
  Modifique los parámetros como se encuentran en la tabla 3.18.

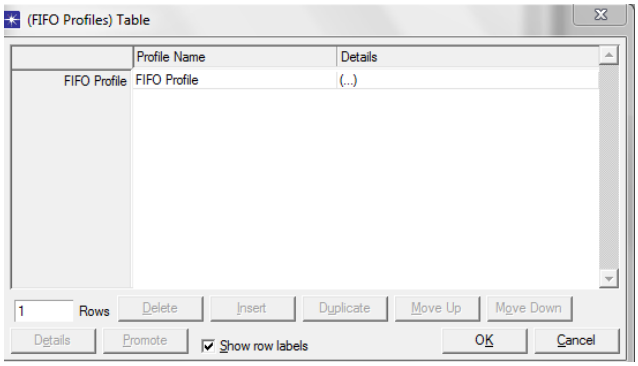
Tabla3.18. Configuración de Streaming Traficc

Name	Star Time Offset (Seconds)	Durations Seconds	Repeatability
Video Conferencing (Streaming Multimedia)	**Distribution Name:** constant **Mean outcome:** 10	End to Profile	Once at star time

Autores

3.6 Configuración de QoS: Configure **QoS Attribute Config**, se oprime click sobre este icono y seleccione **Edit Attributes**; busque la opción **FIFO Profiles,** oprima click sobre **Standard Schemes**, busque **edit,** aparece una tabla como se muestra en la figura 3.10 y agregue **1 fila (rows).**

Figura 3.10. Configuración del perfil FIFO



Saldrá una ventana que tiene como Profile Name, **FIFO Profile** y en **Details**, que viene con la opción **Default,** se buscara la opción **edit** y aparece la tabla 3.19, donde se modifican las siguientes características:

Tabla3.19. Detalles de QoS

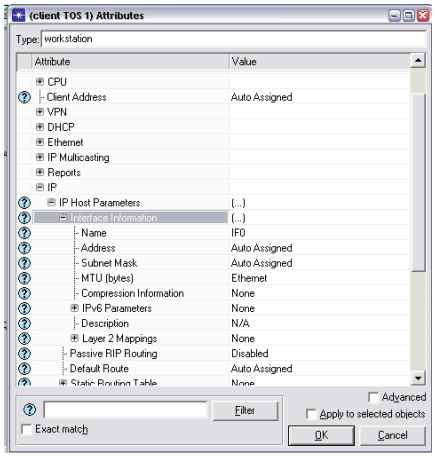
Maximum Queue Size (pkts)	500
RED Paramenters	Disabled

Autores

Finalice oprimiendo click en **OK¸** para realizar cambios.

3.7 Configuración de los clientes IPv4: Ubíquese en **Client TOS1,** y realice click derecho, seleccione **edit atributes**; ahí encontrara información de la estación. En la opción **IP** luego **IP Host Parameters,** posteriormente abra la opción **Interface Information,** despliegue todo el menú, como se muestra en la figura 3.11.

Figura 3.11. Configuración de client TOS 1.



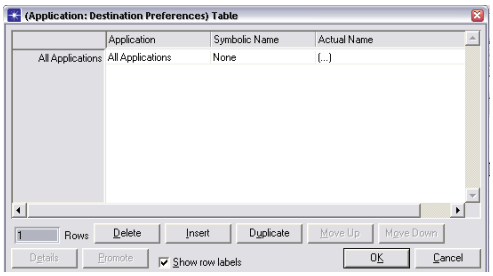
En esta tabla se modifica:

- **Address,** oprimiendo click sobre la opción **Auto Assigned,** y en **edit** asigne una nueva dirección IP **192.0.2.1**
- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne 255.255.255.0
- **MTU(bytes),** para esta estación debe estar en **Ethernet.**

Para guardar cambios realice click en **OK.**

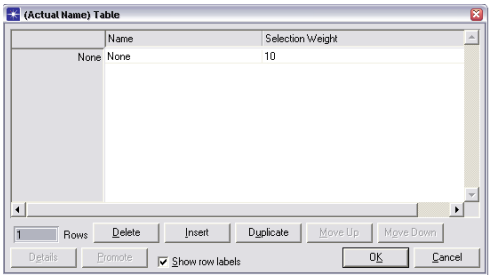
Además se deben configurar las aplicaciones de **Client** ; en la misma tabla de **Edit Attributes**, despliegue la opción **Applications,** diríjase a **Application: Destination Preferences** que por defecto tiene valor **None,** busque la opción **Edit,** y aparecerá tabla 3.12, como la siguiente en donde deberá agregar **1 fila (rows).**

Figura 3.12. Preferencias de Destino



Modifique **Symbolic Name,** que viene con la opción **None** por **Video Destination,** y en **Actual Name** oprima click sobre **(…)** donde aparece la tabla 3.13 en la cual deberá agregar **1 fila (rows).**

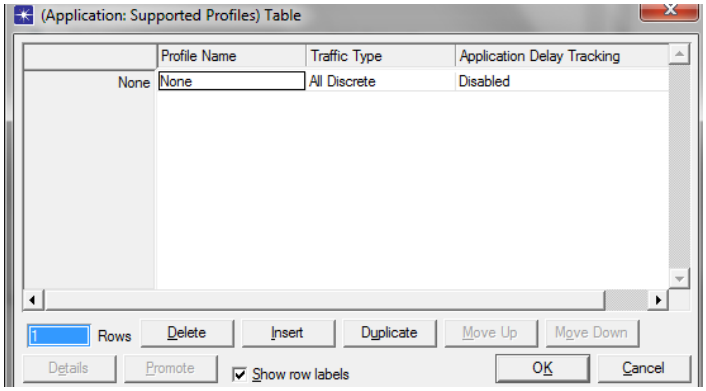
Figura 3.13. Configuración del nombre actual



En **Name** que tiene por defecto el valor **None,** busque la opción **edit**, coloque **s1** y en **Selection Weight** coloque el valor de **100**. Finalice oprimiendo **OK,** para guardar cambios.

En la misma tabla de **Edit Attributes**, se despliega el menú **Applications,** ahora se modifica **Application: Suported Profiles** que tiene por defecto el valor **None,** busque la opción **Edit ,** y aparecerá la tabla 3.14, como la siguiente en donde deberá agregar **1 fila (rows).**

Figura 3.14. Aplicaciones del Perfil Admitido



Se modificara el **Profile name** que tiene **None** por **Background Traffic**, además el **Traffic Type** debe estar en la opción **All discrete** y **Application Delay Tracking** debe estar **Disabled,** finalice oprimiendo **OK** para realizar cambios.

Dado que el **Client ToS 3** es **IPv4,** se realizan los mismos pasos anteriores, pero modificando la siguiente información.

Forma rápida de configuración;

- **IP→ IP Host Parameters → Interface Information** como se muestra en la tabla 3.20.

Tabla3.20. Interfaz de Información Client ToS 3

	Client TOS 2
Address	192.0.2.2
Subnet mask	255.255.255.0
MTU(bytes)	Ethernet

Autores

- **Applications → Application: Destination Preferences** (Agregar 1 Rows), como se muestra en la table 3.21.

Tabla3.21. Preferencias de Destino Client ToS 3

Application	**Symbolic Name**	**Actual Name (agregar 1 rows)**	
All Aplication	Video Destination	**Name:** s3	**Selection Weigth:** 100

Autores

- **Applications → Application: Supported Profiles (**Agregar 1 Rows), como se muestra en la table 3.22.

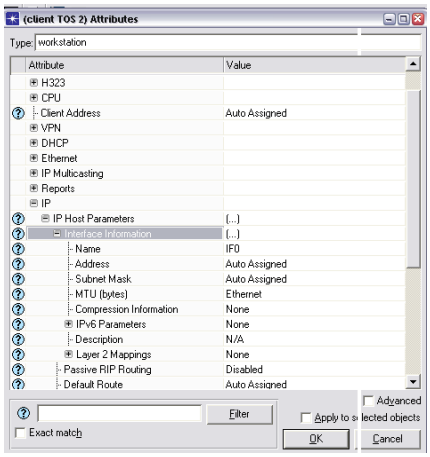
Tabla3.22. Soporte de Perfil habilitado del Client ToS 3

Profile name	Traffic Type	Application Delay Tracking
Excellent Effort Traffic	All Discrete	Disabled

Autores

3.8 Configuración de los clientes IPv6: Luego se configurar el **Client ToS 2** y **4** de la siguiente manera: Ubíquese en **Client TOS 2,** y realice click derecho, seleccione **edit atrributes**; ahí encontrara información de la estación. Despliegue la opción **IP** luego **IP Host Parameters,** posteriormente abra la opción **Interface Information** como se muestra en la figura 3.15.

Figura 3.15. Atributos ToS 2



En esta tabla se modifica:

- **Address,** oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne una nueva dirección IP por **192.0.2.5**

- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne 255.255.255.0
- **MTU(bytes),** debe estar en **Ethernet.**

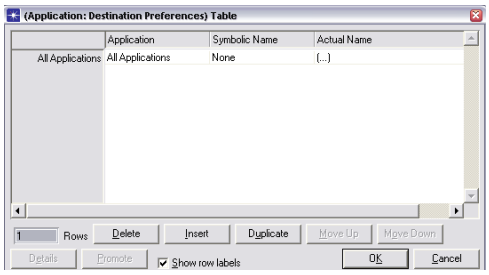
Además en **IPv6 Parameters** oprimiendo click sobre el icono (+) se modificara algunos parámetros:

- **Link Local Address** que se encuentra en la opción **Not Active ,** asigne **Default EUI-64**
- **Global Address (es)** despliegue el icono (+), y encontrara la opción **Not Active,** cambie **Address** que se está en **Not Active,** en **edit** por **2000:0:C000:200::5**, y **Address Type** debe te **Nnre on EUI-64.**

IP, IP Host Parameters en la opción **IPv6 Default Route** que se encuentra en **Auto Assigned,** se asigna la dirección **2000:0:C000:200::4**.

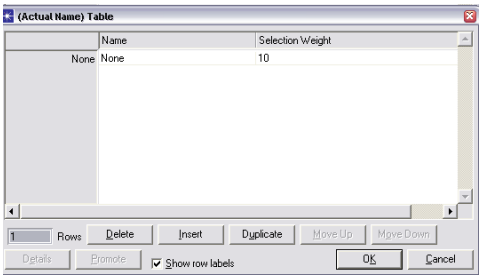
Despliegue el menú de opción **Applications** encontrara **Application: Destination Preferences** que por defecto tiene valor **None** busque la opción **Edit,** y aparecerá la figura 3.16, como la siguiente en donde deberá agregar **1 fila (rows).**

Figura 3.16. Destino de Preferencia ToS 2



Modifique **Symbolic Name,** que viene con la opción **None** por **Video Destination,** y en **Actual Name** oprima click sobre **(…)** donde aparece la figura 3.17, en la cual deberá agregar **1 fila (rows).**

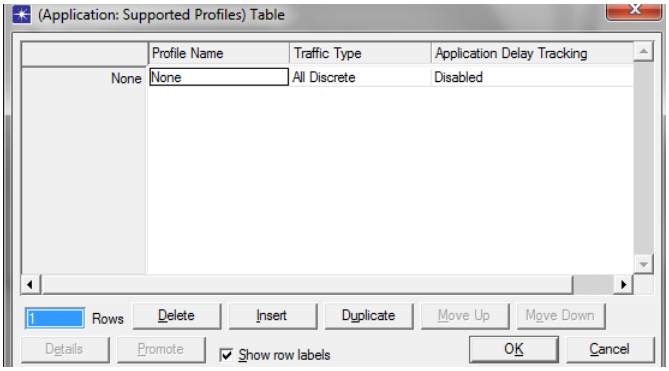
Figura 3.17. Symbolic Name



En **Name** que tiene por defecto el valor **None,** busqué la opción **edit**, coloque **s2** y en **Selection Weight** coloque el valor de **100**. Finalice oprimiendo **OK,** para guardar cambios.

En la misma tabla de **Edit Attributes**, se despliega el menú **Applications,** ahora se modifica **Application: Suported Profiles** que tiene por defecto el valor **None,** busque la opción **Edit ,** y aparecerá la figura 3.18, como la siguiente en donde deberá agregar **1 fila (rows).**

Figura 3.18. Aplicaciones del Perfil Admitido ToS 2



Se modificarà el **Profile name** que tiene **None** por **Standard Traffic**, además el **Traffic Type** debe estar en la opción **All Discrete** y **Application Delay Tracking** debe estar **Disabled,** finalice oprimiendo **OK** para realizar cambios.

Reaizar los pasos anteriores al **Client TOS 4** pero modificando los siguientes valores:

- **IP→ IP Host Parameters → Interface Information** como se muestra en la tabla 3.23.

Tabla3.23. Interfaz de Información Client ToS 4

	Client TOS 4
Address	192.0.2.3
Subnet mask	255.255.255.0
MTU(bytes)	Ethernet

Autores

- **IP→ IP Host Parameters→ Interface Information→ IPv6 Parameters**: Para cambiar Link Local Address, Global Address (es) (Address, Address Type). Como se muestra en la tabla 3.24.

Tabla3.24.Interfaz de Información Client ToS 4

	Client TOS 4
Link local address	Default EUI-64
Global address (es) **Address:** **Address Type:**	 **2000:0:c000:200::3** Non EUI-64
IPv6 Default Route	**2000:0:c000:200::4**

Autores

- **IP→ IP Host Parameters→ IPv6 Default Router**. Como se muestra en la tabla 3.25.

Tabla3.25. Dirección del router Client ToS 4

IPv6 Default Route	**2003:1:1::1**

Autores

- **Applications → Application: Destination Preferences** (Agregar **1 fila (rows)).** Como se muestra en la tabla 3.26.

Tabla3.26 Preferencias de Destino Client ToS 4

Application	Symbolic Name	Actual Name (agregar 1 rows)	
All Aplication	Video Destination	**Name:** s4	**Selection Weigth:** 100

Autores

- **Applications → Application: Supported Profiles (**Agregar 1 **filas (rows)**). Como se muestra en la tabla 3.27.

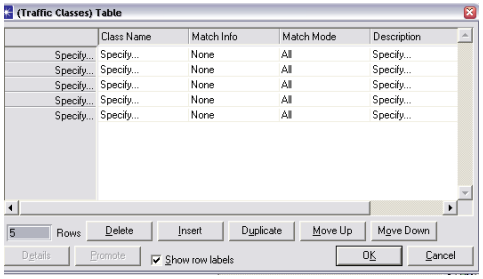
Tabla3.27 Soporte de Perfil habilitado del Client ToS 4

Profile name	Traffic Type	Application Delay Tracking
Streaming Traffic	All Discrete	Disabled

Autores

3.9 Configuración de los routers: Para configurar el **Router A** oprima click derecho sobre él, elija **Edit attributes**, ingrese a **IP** , posteriormente despliegue el menú de **IP QoS Parameters,** ubique la opción **Traffic Classes** que tiene como valor **None,** seleccione **edit** y aparece una ventana como en la figura 3.19, agregue **5 filas (rows)**.

Figura 3.19. Clases de tráfico



Edite la primera fila de la tabla colocando lo siguiente: **Class Name,** tendrá el nombre de **default**, en la opción **Match Info** busque **edit**, oprimir sobre este, aparece una nueva tabla donde se agrega **1 fila (rows)** y se modifica la opción **Match Property** que viene por defecto con el nombre de **Packet** por **Precedence**. Seguidamente **Match Condition** tendrá habilitado la opción **Equals** y **Match Value** tendrá un valor de **0**. Finalice oprimiendo **OK** para realizar cambios.

Para las siguientes filas, se realiza el mismo procedimiento, pero cambia la información como se muestra en la tabla 3.28.

Tabla3.28.Clases de Trafico Router A

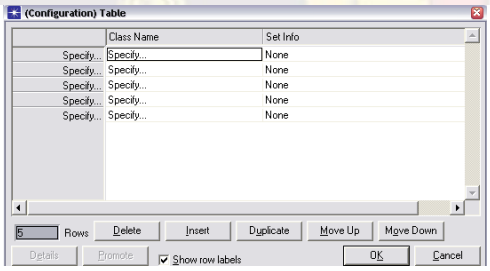
Class Name	Match Property	Match Condition	Match Value
Class 1	ACL	Equals	client TOS 1
Class 2	ACL	Equals	server TOS 2
Class 3	ACL	Equals	server TOS 3
Class 4	ACL	Equals	client TOS 4

Autores

Finalice oprimiendo **OK** para guardar cambios y de nuevo queda en la tabla de **Attibutes.**

Ahora se ingrese a configurar la opción **Traffic Policies** desplegando el menú aparece la opción llamada **Number of Rows**, que viene con el valor de cero (0), coloque este valor en **1**. Aparece una nueva línea llamada **Specify** abra todo su menú y ubique **Policy Name** y al lado en la opción **Specify** coloque este nuevo nombre **my_policy.** En la opción **Configuration** que se encuentra con el valor de **None,** busque **Edit** y parece una tabla como se muestra en la figura 3.20, de la siguiente manera y agregue un **5 filas (rows).**

Figura 3.20. My policy



Edite la primera fila de la tabla colocando lo siguiente: **Class Name,** tendrá el nombre de **default**, en la opción **Set Info** busque **edit**, oprimir sobre este, aparece una nueva tabla donde se agrega **1 fila (rows)** y se modifica la opción **Set Property** donde especifica la opción **MDRR Profile.** Seguidamente **Set Value** con **default**. Finalice oprimiendo **OK** para realizar cambios.

Para las siguientes filas, se realiza el mismo procedimiento, pero cambia la información como se muestra en la tabla 3.29.

Tabla3.29.Configuración MDRR

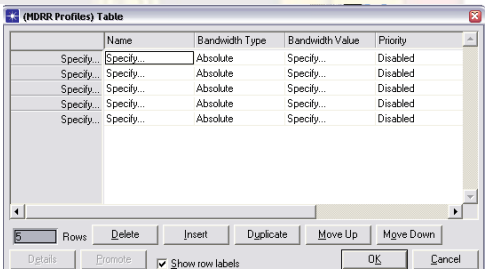
Class Name	Set Property	Set Value
Class 1	MDRR Profile	Q1
Class 2	MDRR Profile	Q2
Class 3	MDRR Profile	Q3
Class 4	MDRR Profile	Q4

Autores

Finalice oprimiendo **OK** para guardar cambios y de nuevo queda en la tabla de **Attibutes.**

- Ingrese a **IP→ IP QoS Parameters→MDRR Profiles**, que tiene como valor **None,** busque **Edit**, aparece una tabla como la figura 3.21, donde debe agregar **5 filas (rows)**.

Figura 3.21. Perfiles MDRR



Edite colocando la información de la tabla 3.30.

Tabla 3.30.Perfiles MDRR Client ToS

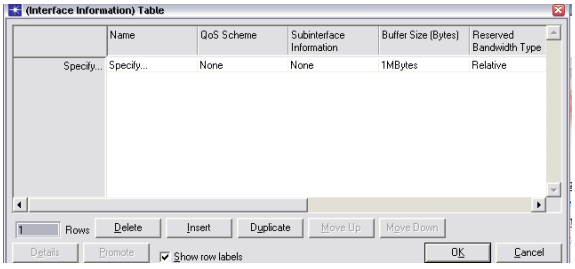
Name	Bandwidth Type	Bandwidth Value	Priority
default	Relative	1	Disabled
Q1	Relative	10	disabled
Q2	Relative	20	disabled
Q3	Relative	30	disabled
Q4	Relative	40	disabled

Autores

Finalice oprimiendo **OK** para guardar cambios

Despliegue **IP,** luego abra la opción **IP QoS Paramenters** modifique **Interface Information** que tiene un valor de **None,** seleccione **edit** y aparece la figura 3.22, de siguiente manera y agregue **1 fila (rows).**

Figura 3.22. Interfaz de la información del Router A

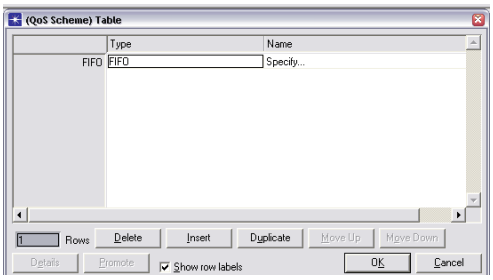


Además modifique lo siguiente:

Name, que se encuentra con **Specify** modifique por **IF0, Maximum Reserved Bandwidth** seleccione **edit** y coloque este valor en **98, QoS Scheme** , que tiene

el valor de **None,** seleccione **edit,** aparece la figura 3.23, como la siguiente**.** Donde debe agregar **1 fila (rows).**

Figura 3.23. Régimen Qos



En **Type** seleccione **Outbound Traffic Policy** y en la opción **Name,** seleccione **my_Policy**, finalice oprimiendo **OK** para realizar cambios.

En el mismo **Router A** en la opción **Editt Attributes,** despliegue **IP,** luego en la abra la opción **IP Routing Parameters,** ubíquese en **Interface Information (10rows)** y realice click en **(…)** y aparecerá una tabla para editar **Address**, que se encuentran en **Auto Assigned,** busque **edit** para colocar las nuevas direcciones.

Forma rápida de configuración:

- **IP→ IP Routing Parameters→ Interface Information (10rows):** Para cambiar Address y Subnet Mask, modifique los parámetros de la tabla 3.31.

Tabla3.31. Configuracion de los parámetros de enrutamiento Router A

	IF0	**IF8**
Address	192.0.3.1	192.0.2.4
Subnet Mask	255.255.255.0	255.255.255.0

Autores

Finalice oprimiendo OK para guardar cambios.

- **IP→IP Routing Parameters→ Loopback Interface** oprima click en **None,** busque **edit,** aparece una ventana, en la parte inferior **(rows)** agregue el

número 1 y realice los siguientes cambios en la tabla oprimiendo en la opción **edit** de cada casilla:

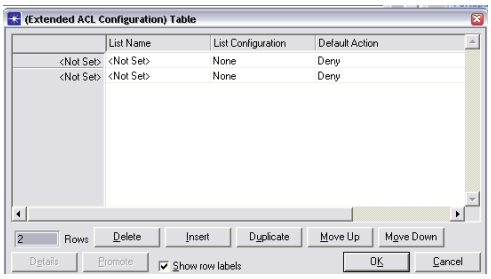
Tabla3.32.Configuración de los parámetros del Loopback

Name	Loopback
Address	192.0.4.1
Subnet Mask	255.255.255.0
Routing Protocol(s)	Enabled (RIP)

Oprima click sobre OK para realizar cambios.

- En el menú **IP→IP Routing Parameters→ Extended ACL Configuration** que se encuentra configurada con **None,** busque **Edit** y aparece la figura 3.24 y agregue **2 filas (rows):**

Figura 3.24. Configuración ACL



Modifique los parámetros de la tabla 3.33.

Tabla3.33.Configuración de los parámetros de ACL

List Name	List Configuration
client TOS 1	Seleccione Edit, y agregue 1 Rows Term: 10 Action:Permit Protocol: Not set Source IP Address: 192.0.2.1 Wildcard/Subnet Mask: host
server TOS 3	Seleccione Edit, y agregue 1 Rows Term: 10 Action:Permit Protocol: Not set Destination IP Address: 192.0.1.3 Wildcard/Subnet Mask: host

Autores

En el mismo **Router A**, en la opción **IP,** seguido de **IPv6 Parameters,** se encuentra **Interface information,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** que se encuentra en cero (0), edite el número 2.

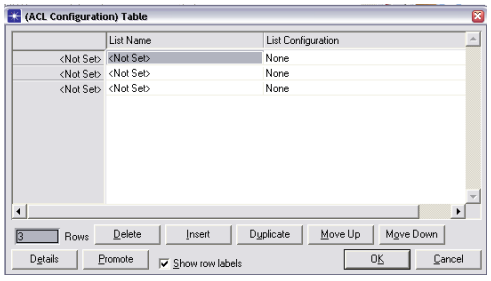
- Abra la opción **IF0** y coloque lo siguiente, **Link local address** en **Default EUI-64,** además despliegue el menú de **Global Address (es)** oprimiendo en el icono (+) y oprima click en **(…)** , busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que se encuentra en **Not Active** busque **edit;** coloque **2000:0:C000:300::1,** además **Address type** debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. El **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng.**
- Luego abra la otra opción **IF0**, donde se encuentra **Name** en **IF0**, busque **IF8** y colóquelo, automáticamente cambia el nombre. Posteriormente en la opción **Link local address** en **Default EUI-64,** además en **Global Address (es)** oprima click en **None** y busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit** y coloque **2000:0:C000:200::4,** además

Address type debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. El **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng.**

- Ahora bien, en la opción **IP,** seguido de **IPv6 Parameters,** se encuentra **Loopback Interfaces,** oprima click en **(+),** busque la opción **Number of Rows** y asigne **1,** posteriormente despliegue el menú de **Loopback ,** edite lo siguiente, **Link- local Address,** asigne **Default EUI-64,** despliegue el menú **Global Address (es)** y oprima click sobre **(…)** y examine la opción **edit,** donde aparece una ventana, la cual editara una fila **(1 Rows),** coloque los siguientes datos: **Address, 2000:0:C000:400::1, y Address type, EUI-64** Para finalizar oprima en la tabla **OK,** y **Routing Protocol (s)** debe tener asignado el valor **RIPng.**

- En la misma tabla de Atributos del Router A, ahora se configura la **Lista de Control de Acceso (ACL).** En la opción **IP,** seguido de **IPv6 Parameters,** se encuentra **ACL Configuration** que tiene como valor **None,** seleccione **edit,** aparece la figura 3.25, de la siguiente manera, donde se agregan **3 filas (rows).**

Figura 3.25. Lista de control de acceso ACL



Modifique los parámetros de la tabla 3.34.

Tabla3.34 Configuración de los parámetros IPv6 de ACL

List Name	List Configuration
match all	Seleccione Edit, y agregue 1 Rows Action:Permit Protocol: Not set Source Prefix/Length: Any
server TOS 2	Seleccione Edit, y agregue 1 Rows Action:Permit Protocol: Not set Source Prefix/Length: Any Destination Prefix/Length: 2000:0:C000:100::5
client TOS 4	Seleccione Edit, y agregue 1 Rows Action:Permit Protocol: Not set Source Prefix/Length: 2000:0:C000:200::3 Destination Prefix/Length: Any

Autores

Finalice oprimiendo click sobren **OK,** en la ventana de los atributos para realizar cambios**.**

Ahora se procede a configurar el **Router B,** oprima click derecho sobre este, busque la opción **editt Attributes,** despliegue **IP,** luego en la abra la opción **IP Routing Parameters,** ubíquese en **Interface Information (10 rows)** y realice click en **(…),** aparecerá una tabla para editar las **direcciones (Address)** , que se encuentran en **Auto Assigned,** busque **edit** para colocar las nuevas direcciones.

Forma rápida de configuración:

- **IP→ IP Routing Parameters→ Interface Information (10rows):** Para cambiar Address y Subnet Mask.

  Modifique los parámetros de la tabla 3.35.

Tabla3.35. Configuración de los parámetros de enrutamiento Router B

	IF1	**IF8**
Address	192.0.3.2	192.0.1.1
Subnet Mask	255.255.255.0	255.255.255.0

Autores

Luego oprima click en **OK.**

Vuelva al menú de atributos, en **IP** despliegue la opción **IP Routing Parameters**, en la línea de **Loopback Interface** oprima click en **None** y seleccione **edit,** aparece una ventana, y en la parte inferior agregue **(1 rows)**. Realice los siguientes cambios en la tabla 3.6, oprimiendo en la opción **edit** de cada casilla:

Tabla3.36. Configuración de los parámetros de enrutamiento del Loopback

Name	loopback
Address	192.0.5.1
Subnet Mask	255.255.255.0
Routing Protocol(s)	Enabled (RIP)

Autores

Finalice oprimiendo **OK,** para realizar cambios.

En la misma tabla de atributos, en la opción **IP,** seguido de **IPv6 Parameters,** se encuentra **Interface Information,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** que se encuentra en cero (0), edite el número 2.

- Abra la opción **IF0** y coloque lo siguiente, **Link local address** en **Default EUI-64,** además despliegue el menú de **Global Address (es)** oprimiendo

en el icono (+), oprima click en **(…)** y busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit;** coloque **2000:0:C000:300::2,** además **Address type** debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. En **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng.**

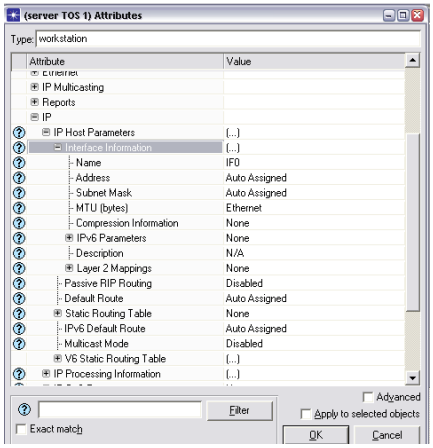
- Luego abra la otra opción **IF0**, y donde se encuentra **Name** en **IF0**, busque **IF8** y colóquelo, automáticamente cambia el nombre. Posteriormente en la opción **Link local address** sitúela en **Default EUI-64,** además en **Global Address (es)** oprima click en **None** y busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que está en **Not Active** busque **edit** y coloque **2000:0:C000:100::1,** además **Address type** debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. En **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng.**

Ahora se procede a configurar el **lookback**, en la opción **IP,** seguido de **IPv6 Parameters,** se encuentra **Loopback Interfaces,** oprima click en **(+),** y busque la opción **Number of Rows** y asigne el valor de **1,** posteriormente despliegue el menú de **Loopback ,** edite lo siguiente, **Link local Address** en **Default EUI-64,** despliegue todo el menú de **Global Address (es)** y oprima click sobre **(…)** y examine la opción **edit,** donde aparece una ventana, y agregue **1 rows,** coloque los siguientes datos: **Address, 2000:0:C000:500::1, y Address type, EUI-64** Para finalizar oprima en la tabla **OK,** y **Routing Protocol (s)** debe tener asignado el valor **RIPng.** Finalice oprimiendo click en ventana de los atributos para realizar cambios.

3.10 Configuración de los Server: Ubíquese en **Server TOS 1,** realice click derecho, seleccione **edit atrributes**; ahí encontrara información de la estación.

Ingrese a la opción **IP** luego **IP Host Parameters,** posteriormente abra la opción **Interface Information** oprimiendo click sobre el icono (+) como se muestra en la figura 3.26.

Figura 3.26. Atributos del Server TOS 1



En esta tabla se modifica lo siguiente:

- **Address,** oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne un nueva dirección IP por **192.0.1.2**
- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned** y en **edit** asigne 255.255.255.0
- **MTU(bytes),** para esta estación debe estar en **Ethernet.**

Además en **IP→IP Host Parameters→Interface Information→ IPv6 Parameters,** oprima click sobre el icono (+) y modifique los siguientes parámetros:

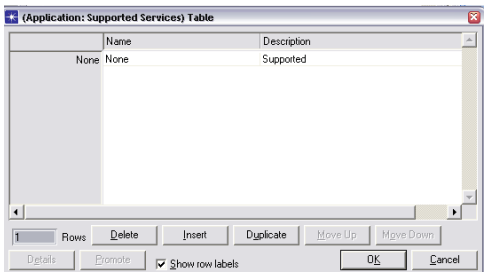
- **Link Local Address** que se encuentra en la opción **Not Active ,** asigne **Default EUI-64**
- **Global Address (es)** despliegue el icono (+), y encontrara la opción **Not Active,** abra esta opción y cambie la dirección **(Address)** que se está en **Not Active,** en **edit** por **2000:0:C000:100::2**, y **Address Type** debe estar **Non EUI-64**

IP Host Parameters en la opción **IPv6 Default Route** que se encuentra en **Auto Assigned,** se asigna la dirección **2000:0:C000:100::1**, Por último oprima **OK** para guardar los cambios realizados.

Ahora realice nuevamente click derecho sobre **server TOS 1,** seleccione **edit attributes,** ingrese a **Client Address,** que se encuentra con la opción **Auto Assigned,** busque **edit** y asigne **s1.**

Se deben configurar el tipo de servicio que soporta, ingrese a **Applications,** despliegue todo su menú, y ubique la opción **Application: Supported Services** que tiene como valor **None,** busque **edit** e inmediatamente saldrá una ventana en la cual se agrega **1 fila (rows).** Como se muestra en la figura 3.27.

Figura 3.27.Configuracion del soporte para Server TOS 1



Modifique la aplicación como esta en la tabla 3.37.

Tabla3.37.Configuración del tipo de servicio que soporta Server ToS 1

Name	Description
Video Conferencing (Background)	Supported

Autores

Finalice oprimiendo click en **OK,** para realizar cambios

Los pasos anteriores se repiten para los **Server TOS 2, Server TOS 3 y Server TOS 4.**

Forma rápida de configuración los atributos:

- **IP→ IP Host Parameters→ Interface Information** (Para configurar Address, Subnet mask, MTU(bytes)
- **IP→IP Host Parameters→Interface Information→ IPv6 Parameters** (Para configurar Link Local Address, Global Address (es))
- **IP→IP Host Parameters→IPv6 Default Route**
  - **Client Address**
  - **Applications→ Application: Supported Services**

Modifique los parámetros como están en la tabla 3.38.

Tabla3.38. Configuración de Server ToS 2 , Server ToS 3 y Server ToS 4

	Server TOS 2	**Server TOS 3**	**Server TOS 4**
Address	192.0.1.5	192.0.1.3	192.0.1.4
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0
MTU(bytes)	Ethernet	Ethernet	Ethernet
Link local address	Default EUI-64	Default EUI-64	Default EUI-64
Global address (es) **Address:** **Address Type:**	 2000:0:C000:100::5 Non EUI-64	 2000:0:C000:100::3 Non EUI-64	 2000:0:C000:100::4 Non EUI-64
IPv6 Default Route	**2000:0:C000:100::1**	**2000:0:C000:100::1**	**2000:0:C000:100::1**
Client Address	**s2**	**s3**	**s4**
Applications: Supported services (agregar 1 Rows) **Name:** **Description:**	 Video Conferencing (standartd). supported	 Video Conferencing (excellent effort). supported	 Video Conferencing (streaming multimedia). supported

Autores

3.11 Selección de resultados: En el escenario principal, realice click derecho, seleccione la opción **Choose individual DES statistics,** seleccione lo que se encuentra en la tabla 3.39.

Tabla 3.39. Selección de Resultados

Node Statistics

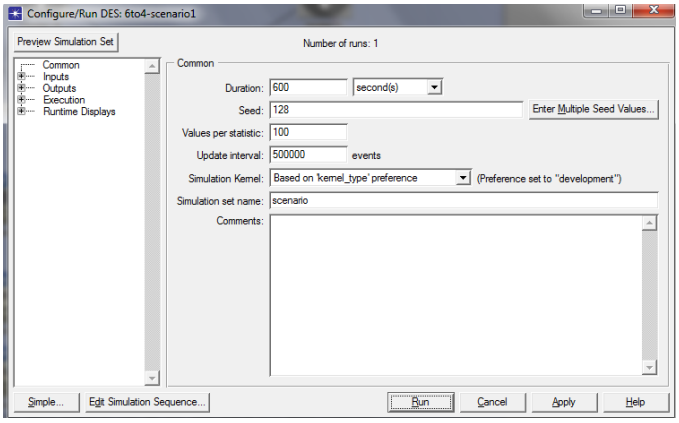
• **IP Interface**
✓ Video Called Party
✓ Video Calling Party
✓ Video Conferencing

Autores

3.12 Realización de simulación: Para llevar a cabo la simulación, realice los siguientes pasos;

- En la barra de herramientas se encuentra el icono RUN  donde aparece una ventana mostrando la duración de la simulación; esta duración se puede modificar para ver mayores intervalos de tiempo. Asigne los siguiente; Duration 600 segundos, seed 128, values per statistics 100, Update interval 100000. Como se muestra en la figura 3.28.

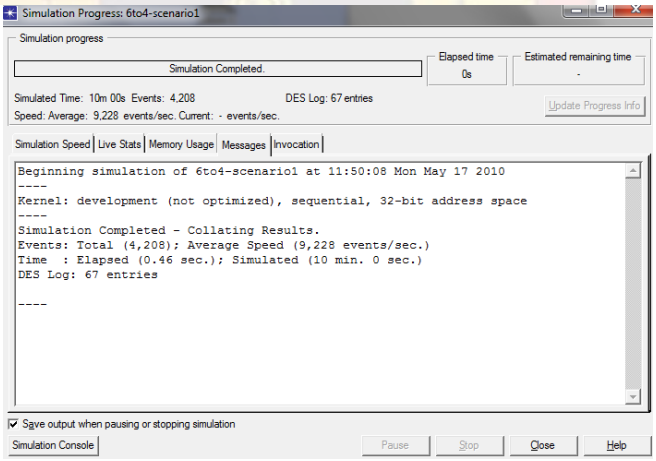
Figura 3.28.Parametrs de la simulación



Después de configurar este parámetro, haga click en **RUN**.

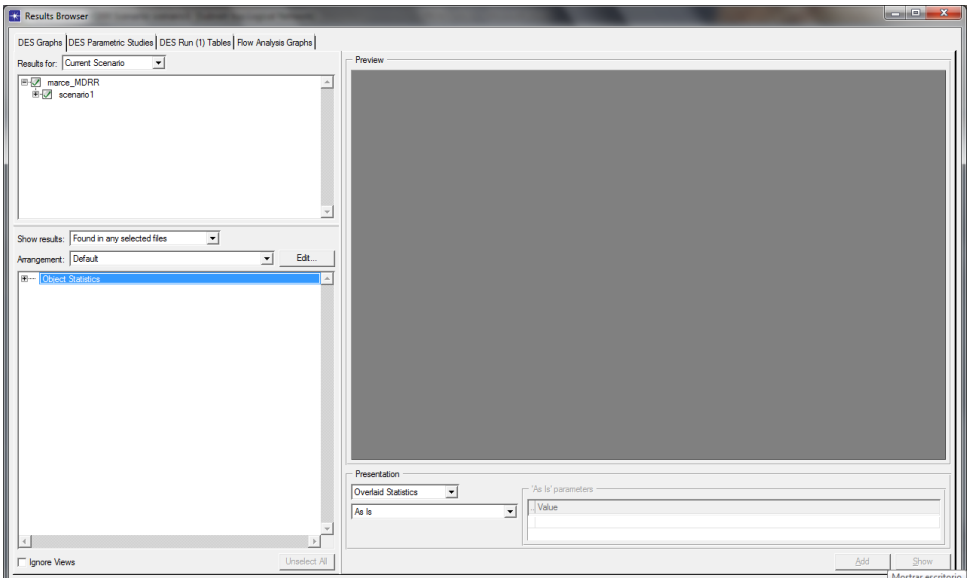
Ahora bien, al terminar el proceso de detección de errores se cierra la ventana en el botón **close y** aparece la figura 3.29.

Figura 3.29.Detector de Errores



3.13 Resultados: Para revisar la tabla de resultados se ingresa al menú **Flow Analysis,** posteriormente se buscara **Results**, se dará click en **View Results** y aparece la figura 3.30 (**Result Browser)**, donde se debe ingresar a la pestana **DES Graphs.**

Figura 3.30. Resultados del Navegador



Para observar la calidad de servicio del tráfico y envió de paquetes (recibidos y enviado) que se encuentra en los client y en los server de la práctica; Ingrese a

Object Static que se encuentra en la parte inferior de la ventana, y desplegué todo el menú para observar las graficas.

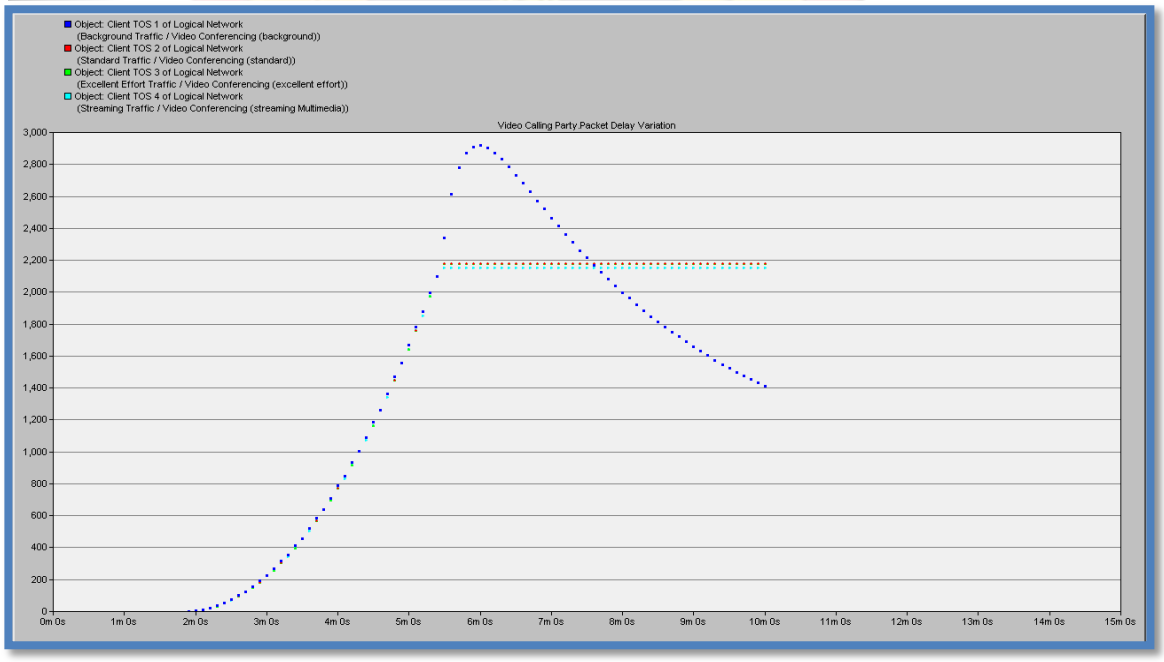
Para visualizar las graficas de forma comparativa, en **Presentation** que se encuentra debajo del espacio gris, debe estar en **Overlaid Statistics.**

Puede observar las siguientes graficas, para un mejor desarrollo de la práctica

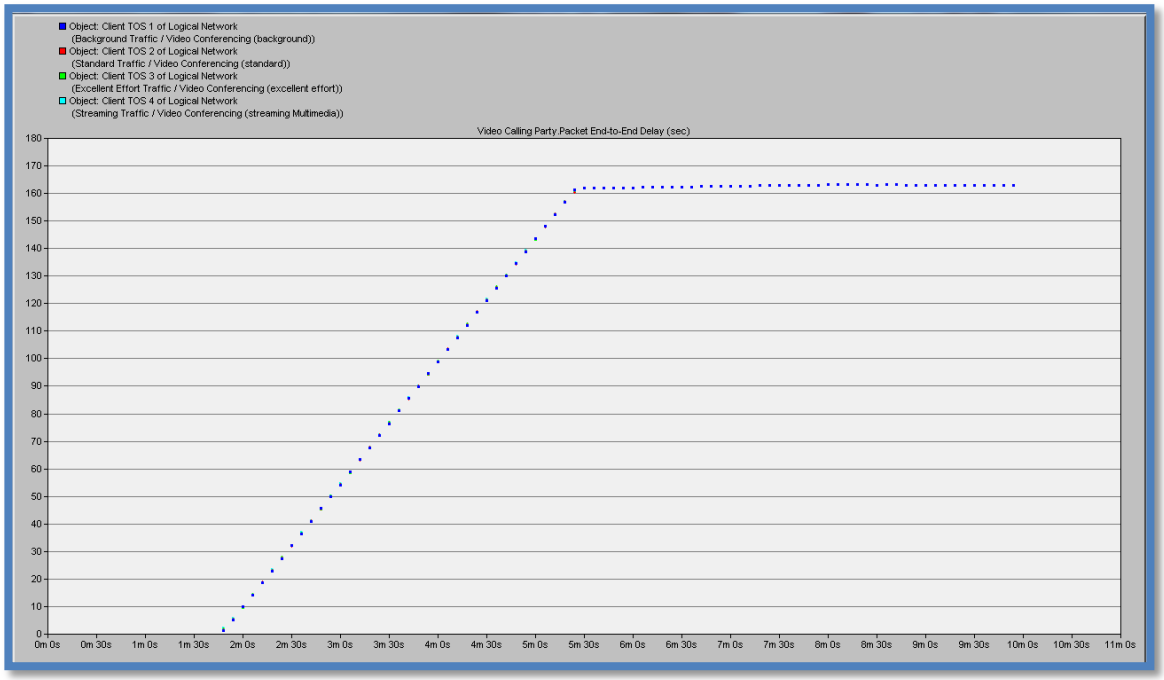
- Despliegue **object statistics**, seleccione de cada Client ToS 1 , Client ToS 2, Client ToS 3 y Client ToS 4, la opción **Video calling Party** y revise los gráficos de Packets Delay Variation, Packect End-to-End Delay.
- Despliegue **object statistics**, seleccione de cada Client ToS 1 , Client ToS 2, Client ToS 3 y Client ToS 4, la opción **Video Conferencing** los gráficos de Packets Delay Variation.
- Gráficos del Router A
- Resultados de los server ToS 1, server ToS 2, server ToS 3 Y server ToS 4. Video Called Party.

A continuación se muestran posibles resultados de la práctica realizada, donde se muestran diferentes parámetros que se están midiendo como calidad de servicio en cada una de las aplicaciones.

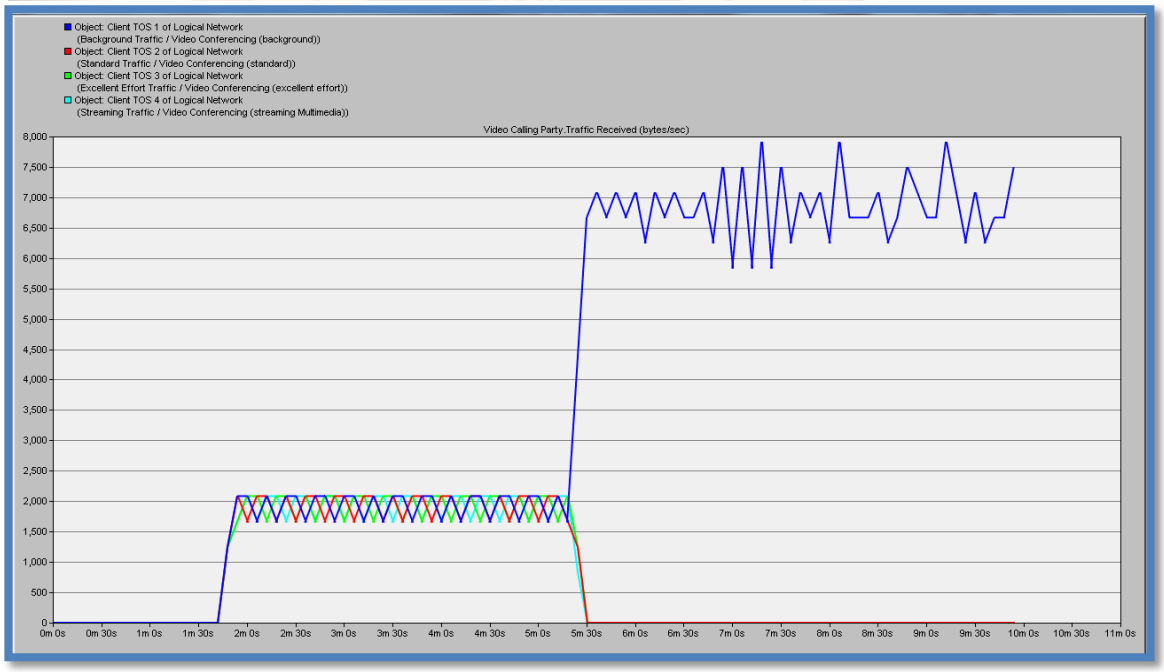
Video calling Party: Packets Delay Variation



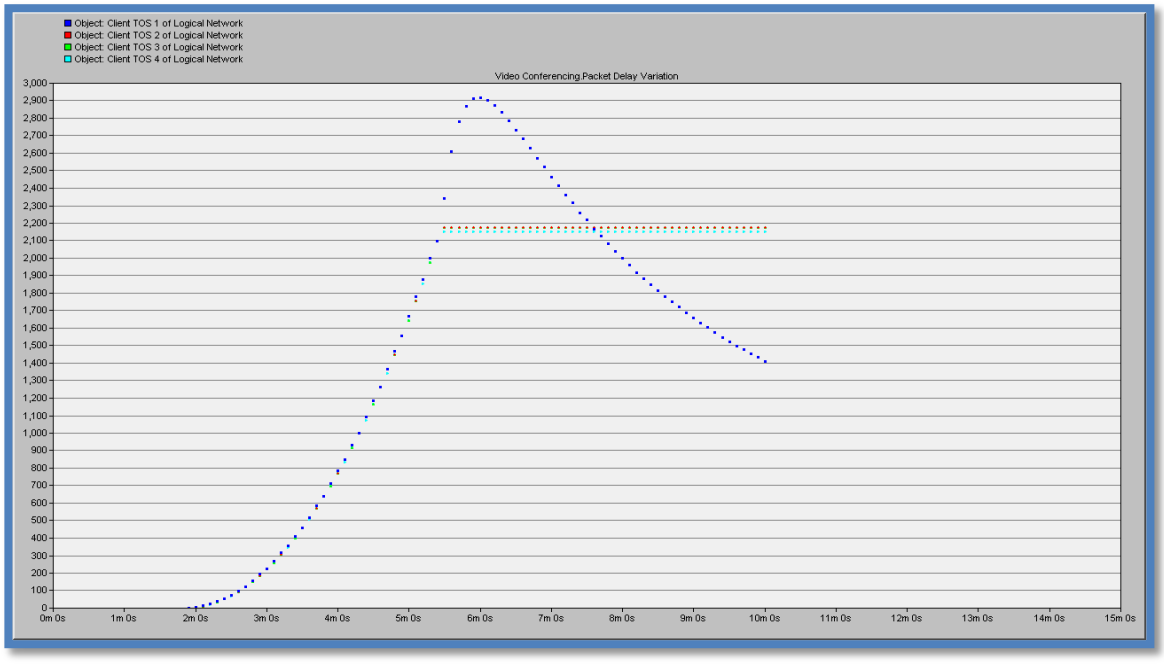
Video calling Party: Packect End-to-End Delay



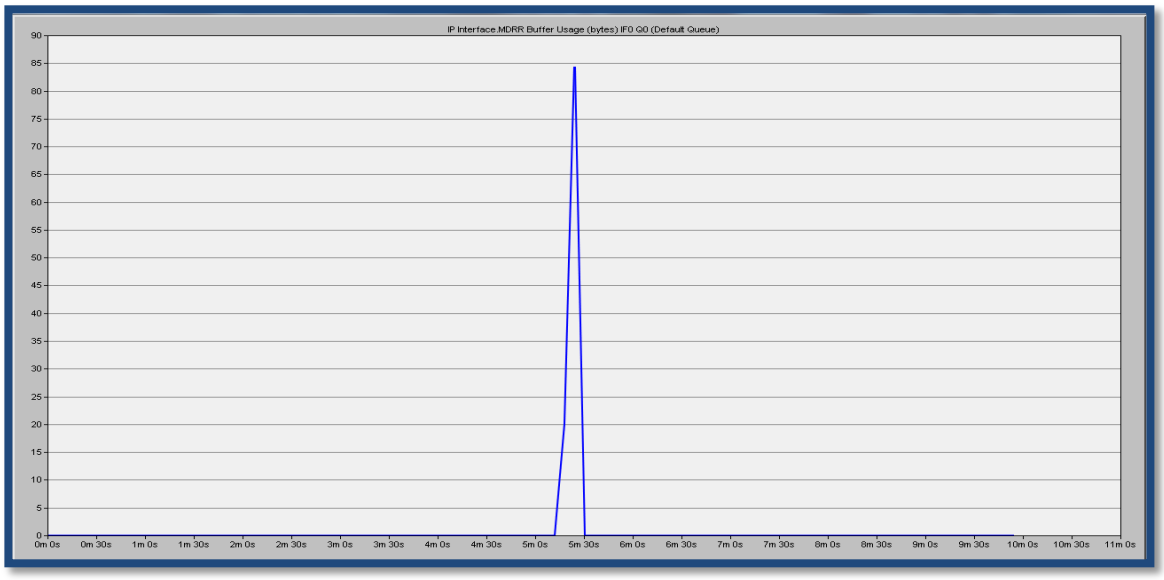
Video calling Party: Traffic Received (bytes/sec)



Video Conferencing: Packet delay Variation

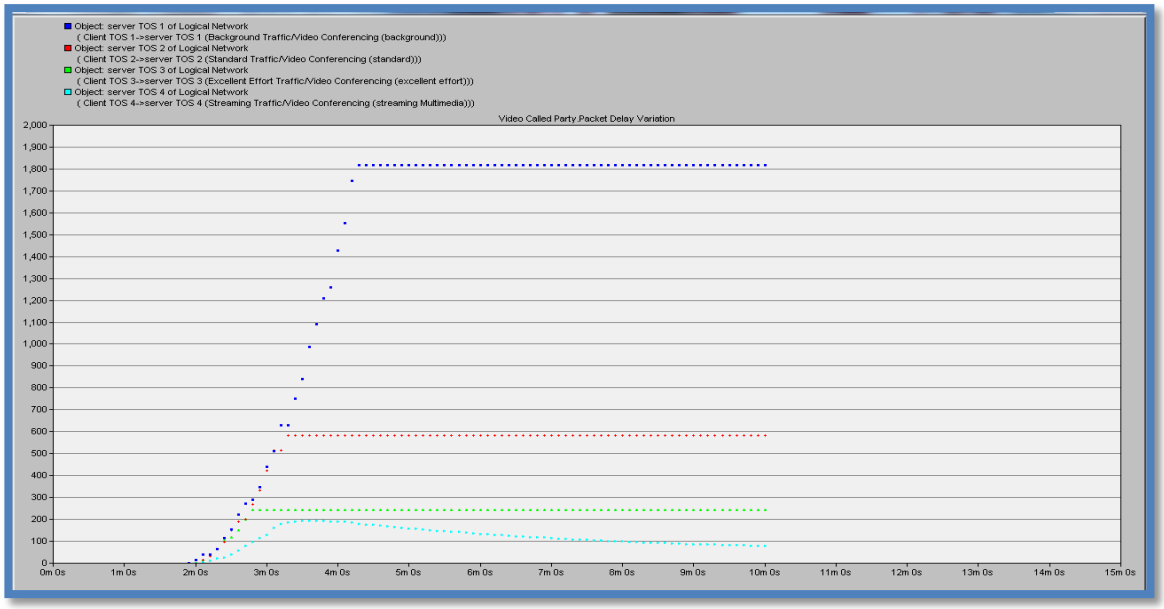


Gráficos del router A: IP Interface. MDRR Buffer Usage (bytes) IF0 Q0 (Default Queue)

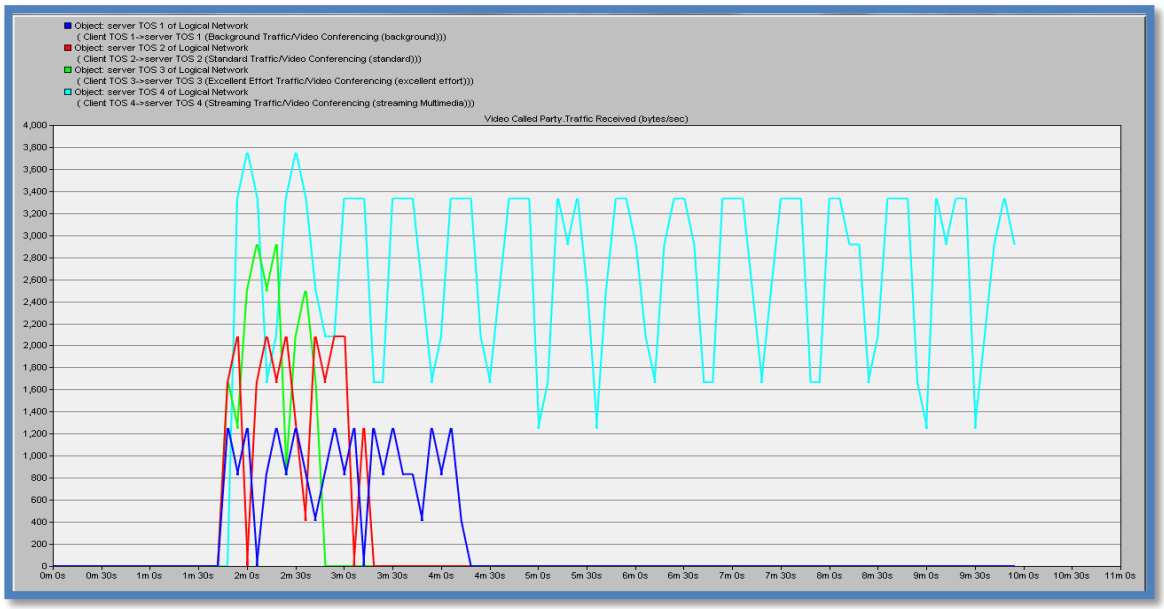


Resultados de los server ToS 1, server ToS 2, server ToS 3 Y server ToS4.

Video Called Party. Packet Delay Variation



Video Called Party. Traffic Received (bytes/sec)



Tarea

En el escenario **Disabled,** realice las siguientes configuraciones, para observar que sucede con las graficas.

Modifique el paso 3.4, cambiándole el **Type of Service,** a las siguientes aplicaciones:

NOMBRE DE LA APLICACION	**Type of Service**
Database Access (Heavy)	Background(1)
Database Access (Light)	Background(1)
File Transfer (Heavy)	Standart (2)
File Transfer (Light)	Standart (2)
Telnet Session (Heavy)	Excellent Effort(3)
Video Conferencing (streaming Multimedia)	Streaming Multimedia(4)
Video Conferencing (excellent effort)	Best Effort (0)
Video Conferencing (Standart):	Best Effort (0)
Video Conferencing (background):	Best Effort (0)

Realice la simulación y observe que cambios nota

Practica N. 4

TITULO: MIPv6

OBJETIVOS

- Conocer la arquitectura y la metodología que tiene IP Movil para utilizar eficientemente dos direcciones IP, una para identificaciones y otra para enrutamiento. Ver el efecto del mecanismo de optimización de la ruta en Ip móvil

1. MARCO TEÓRICO

Movilidad: Se entiende por movilidad a la capacidad que tiene un nodo de una red para mantener la misma dirección IP, a pesar que se desplace físicamente a otra red. Es decir que sin importar su ubicación este puede seguir siendo accesible a través de su misma dirección IP. Sin esta capacidad, los paquetes destinados a un nodo móvil, no podrán llegar a destino mientras dicho nodo, se encuentre alejado de su enlace principal.

Esquemas de agentes de movilidad jerárquicos; que se basan en una estructura jerárquica de Foreign Agents. El nodo móvil registra en su Home Agent la dirección del Foreign Agent que se encuentra en la raíz de la jerarquía de agentes del dominio (Gateway Foreign Agent, GFA). El movimiento entre redes dentro de un dominio se resuelve de manera local, registrándose en el GFA y sin involucrar al Home Agent. Con este esquema trabaja Mobile IP.

Moblie IP nombra a las entidades que participan para poder llevar a cabo la movilidad de los nodos TCP/IP de la siguiente manera:

- Mobile Node (MN): un nodo que puede cambiar su ubicación de acceso, de una red a otra, manteniendo cualquier comunicación y utilizando solo su dirección IP permanente (Home address).
- Care-Of- Address(AOA): Es una dirección IP asociada con el nodo móvil mientras este se encuentra visitando otra subred.

- Foreign Agent Care-Of-Address: es un IP que pertenece a un Foreign Agent que tiene un interfaz en la red externa en donde se encuentra actualmente el nodo móvil.
- Co-located Care-Of-Address: es una IP asignada de manera temporal al nodo móvil, se emplea cuando no existe un Foreign Agent en la red y no puede ser utilizada por mas de un nodo al mismo tiempo.

- Home Agent(HA): un router con una interfaz a la red local, en la cual el nodo móvil ha registrado su COA, de esta manera el HA mantiene información de la situación actual del nodo móvil. Captura los paquetes con destino al nodo móvil y los envía a través de un túnel.
- Foreign Agent(FA): es un router con una interfaz a una red externa, en donde se encuentra de visita el nodo móvil actualmente. Este agente informa al Home Agente de la Care-Of-Address que tiene el nodo móvil en ese momento, actúa como punto de salida del túnel.

Funcionamiento de Movilidad; Mediante un mensaje *Agent Advertisement* tanto el *Home Agent* como los *Foreign Agents* dan aviso de su presencia a cualquier nodo que se encuentre conectado a alguna de sus interfaces.

Cuando los nodos móviles escuchan este mensaje determinan si se encuentran en su red local *(Home Network),* o en una red externa (*Foreign Network*).
Si se encuentran en su red local actúan como cualquier nodo fijo, sin recurrir a las cualidades de *Mobile IP*. Si se encuentran en una red externa, adquieren una *Care-Of-Address*, la cual puede ser tomada de los mensajes *Agent Advertisement*, DHCP, IPCP (Protocolo de Control IP de PPP), o a través de una asignación manual.

Los paquetes enviados al nodo móvil son interceptados por el *Home Agent*, quien los transmite por medio de un túnel hacia la dirección *Care-Of-Address*. En sentido contrario los paquetes son enviados por el nodo, a su destino sin

necesidad de emplear el túnel. En la siguiente figura se muestra el proceso de enrutamiento que realiza *Mobile IP*.[28]

2. DESCRIPCIÓN DEL ESCENARIO

La red IPV6 está compuesta por cuatro puntos de acceso WLAN conectados a través de una nube IP. EL núcleo de red, representado por la nube IP, tiene una latencia de 0,1 segundos. Esto facilita la observación de los diferentes efectos MIPV6 de los mecanismos por el retraso de la aplicación.
MN_A y MN_B se comunican entre sí mediante la ejecución de una aplicación de video muy ligera como una fuente constante de tráfico UDP.

Inicialmente los móviles se colocan en sus redes de origen correspondiente (Home Networks). Entonces el MN_A (Mobile Node A) es servido por el agente de local HA_A (home agent A) y la estación MN_B (Mobile Node B) es servida por el agente de local HA_B (home agent B). Ambos móviles usan MIPV6 para recorrer varios puntos de acceso en la red.
El movimiento realizado por los nodos puede ser descrito de la siguiente manera.

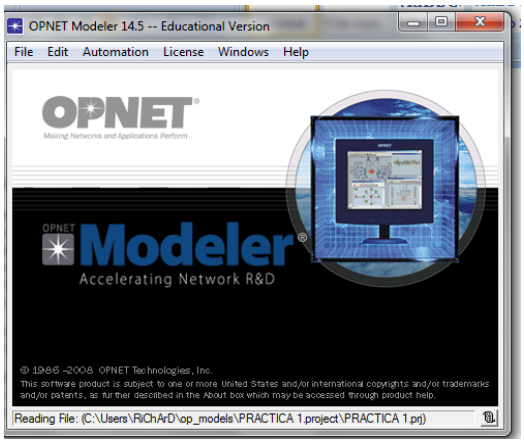
- MN_A: se mueve en una trayectoria anti horaria a través de los cuatro puntos de acceso en la red.
- MN_B: se mueve primero en una trayectoria horaria en los cuatro puntos de acceso en la red.

[28] MOBILE IP, Eugenio Aviluz Ramírez
http://homepage.cem.itesm.mx/raulm/teaching/seminar/notes/Nota_Mobile%20IP.pdf

3. PASOS A SEGUIR

Ejecutar el programa como se muestra en la figura 3.1

Figura 3.1. Interfaz de OPNET



3.1 Creación de un nuevo proyecto: Vaya a la opción **File** de la barra de herramientas y selecciones la opción **New**. A continuación aparecerá una ventana donde se solicita el tipo de proyecto. Seleccione la opción **Project** y luego haga click en **OK**. (**Descripción rápida:** File→ New→ Project → ok).

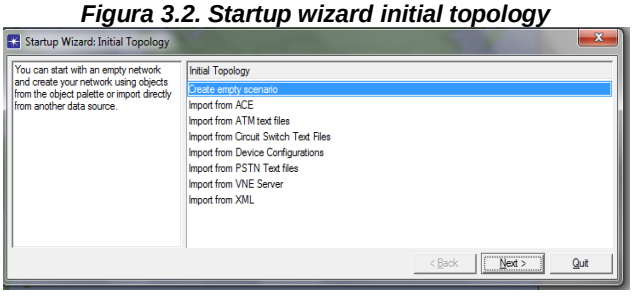
Project name → < mobile_IPv6>

Scenario name→ enabled →ok.

Asegúrese de que se encuentre seleccionada la opción **starup wizard.**

3.2 Configuración del escenario de la red: a continuación aparecerá la figura 3.2, que muestra la ventana inicial del ayudante. Seleccione: (Startup wizard: initial topology → create empty scenario→ next).

Figura 3.2. Startup wizard initial topology



A continuación aparece la opción de selección de la escala de la red. Seleccione: (Campus→ next).

Se debe seleccionar el espacio en cual se va trabajar:(Size→ X span 10, Y span 10, Unit Kilometers→ next)

Ahora aparece el menú de tecnologías disponibles; seleccione las tecnologías: **internet_toolbox, link_PPP, MIPv6_adv** y **mobile_ip** (select Technologies→ internet_toolbox, link_PPP, MIPv6, mobile_ip →next→Finish).

3.3 Creación de la red: Aparece un espacio de trabajo de color azul en el cual se creará la topología; aparecerá una ventana llamada **Object Palette Tree**, allí se desplegaran los iconos de los diferentes dispositivos de las tecnologías que se escogieron, seleccione los siguientes modelos:

Tabla 3.1. Elementos de la red MIPv6

Cantidad	Modelo	Tipo
4	wlan_ethernet_slip4_adv	Fixed Node
2	wlan_wkstn_adv	Mobile Node
1	Profile Config	Fixed Node
1	Application Config	Fixed Node

Autores

Ahora en la opción **Search by name**, de **Object Palette Tree**, busque **ip8_cloud_adv**, y oprima **Find Next** hasta encontrar este modelo y ubíquelo en el área de atrabajo.

A continuación edite los nombres de cada dispositivo como se muestra en la tabla 3.2, oprimiendo click derecho sobre cada icono y seleccionando la opción **Set name**.

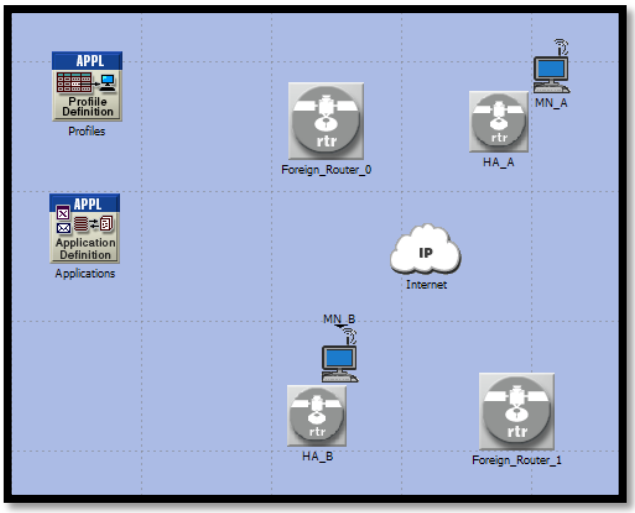
Tabla3.2. Nombres de otros elementos de la red MIPv6

Modelo	Nombre
wlan_ethernet_slip4_adv	Foreign_Router_0
wlan_ethernet_slip4_adv	HA_A
wlan_ethernet_slip4_adv	Foreign_Router_1
wlan_ethernet_slip4_adv	HA_B
wlan_wkstn_adv	MN_A
wlan_wkstn_adv	MN_B
ip8_cloud_adv	Internet
Profile Config	Profiles
Application Config	Applications

Autores

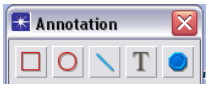
Ahora organice los elementos de la red en la figura 3.3

Figura 3.3. Escenario MIPv6



Agrupe los elementos con la siguiente herramienta; ingrese al menú **Topology,** busque **Open Annotation Palette,** y aparecerá una ventana como se muestra en la figura 3.4, de nombre (**Annotation)**

Figura 3.4. Annotation



Seleccione  y agrupe como se muestra a continuación, posteriormente oprima click derecho sobre cualquier borde del ovalo, e ingrese a **Edit Attributes,** y en **fill,** que se encuentra con la opción **no fill,** activela **fill,** para rellenar el ovalo. También puede cambiarle el color al ovalo, a su gusto. Para guardar cambios oprima en **OK.** Quedara como se muestra en la figura 3.5.

Una los diferentes elementos con enlaces de tipo Link Models **T1** (estos se encuentran en el menú **object palette tree).** Conecté como se muestra en la tabla 3.3.

Figura 3.5 Construcción de sitios MIPv6

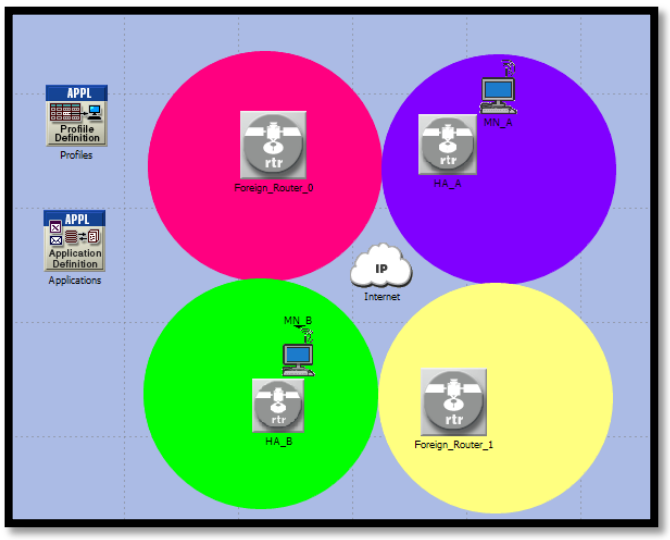


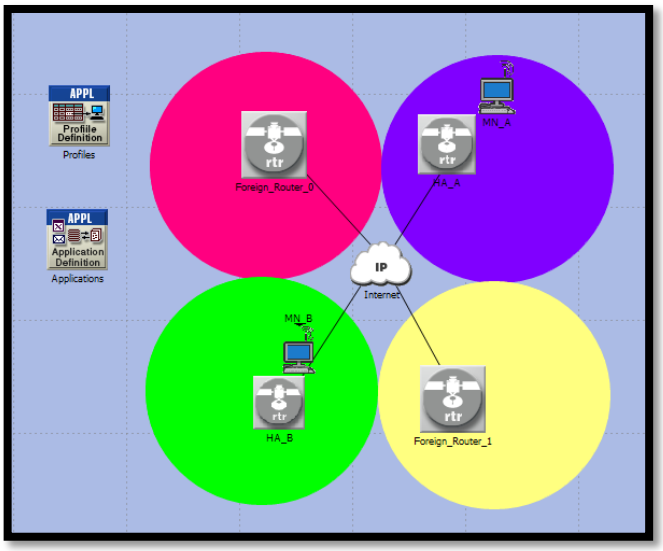
Tabla 3.3. Conexiones de la red MIPv6

Destino	Tipo de Enlace	Fuente
Internet	**PPP T1**	Foreign_Router_0
		HA_A
		Foreign_Router_1
		HA_B

Autores

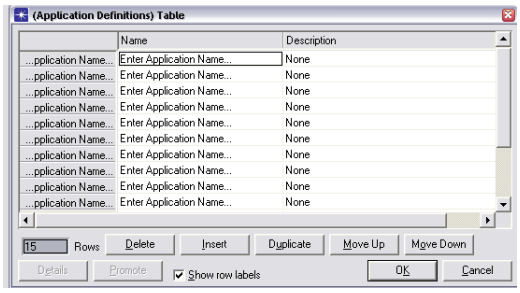
Por lo que la red quedara como se muestra en la figura 3.6

Figura 3.5 Escenario MIPv6 con enlaces



3.4 Configuración de las aplicaciones: Ahora se procede a configurar el modulo **Applications Config**,se oprime click sobre este modulo y seleccione **Edit Attributes**; busque la opción **Application Definitions,** oprima click sobre **None** y seleccione **Edit,** posteriormente saldrá una ventana y en la parte inferior agregue **15 filas (rows),** como se muestra en la figura 3.7.

Figura 3.7. Definición de las aplicaciones



A continuación en cada fila cree las siguientes aplicaciones:

- **Database Access (Heavy):** Busque la opción **edit** de la columna **Description**, aparece una ventana y seleccione **Database** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.4 que deberá quedar con las siguientes especificaciones:

Tabla 3.4. Configuración Database

Transaction Mix (Queries/Total Transactions)	50%
Transaction Interarrival Time(seconds)	**Distribution name:** exponential **Mean outcome:** 12
Transaction Size(bytes)	**Distribution name:** Constant **Mean outcome:** 32768
Symbolic Server Name	Database Server
Type of Service	Best Effort (0)
RSVP Parameter	None
Back- End Custom Application	Not used

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Database Access (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Datebase** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.5 que deberá quedar con las siguientes especificaciones:

Tabla 3.5 Configuración Database Access (Light)

Transaction Mix (Queries/Total Transactions)	50%
Transaction Interarrival Time(seconds)	**Distribution name:** exponential **Mean outcome:** 30
Transaction Size(bytes)	**Distribution name:** constant **Mean outcome:** 16
Symbolic Server Name	Database Server
Type of Service	Best Effort (0)
RSVP Parameter	None
Back- End Custom Application	Not used

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Email (Heavy):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Email** que tiene por defecto el valor **Off,** busque **High Load** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios
- **Email (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Email** que tiene por defecto el valor

Off, busque **Low Load** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**

- **File Transfer (Heavy):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Ftp** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.6 que deberá quedar con las siguientes especificaciones:

Tabla 3.6. Configuración File Transfer (Heavy)

Command Mix (Get/total)	**50%**
Inter-Request Time(Seconds)	**Distribution name:** Exponential **Mean outcome:** 360
File Size(bytes)	**Distribution name:** Constant **Mean outcome:** 50000
Symbolic Server Name	**FTP Server**
Type of service	**Best Effort (0)**
RSVP Parameter	**None**
Back- End Custom Application	**Not used**

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **File Transfer (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Ftp** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.7que deberá quedar con las siguientes especificaciones

Tabla 3.7. Configuración File Transfer (Light)

Command Mix (Get/total)	50%
Inter-Request Time(Seconds)	**Distribution name:** Exponential **Mean outcome:** 3600
File Size(bytes)	**Distribution name:** Constant **Mean outcome:** 1000
Symbolic Server Name	FTP Server
Type of service	Best Effort (0)
RSVP Parameter	None
Back- End Custom Application	Not used

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **File Print (Heavy):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Print** que tiene por defecto el valor **Off,** busque **Color Prints** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **File Print (Light):** Busque la opción **edit**, de la columna **Description,** aparece una ventana y seleccione **Print** que tiene por defecto el valor **Off,** busque **Text File** y asigne este valor. Finalice oprimiendo **OK,** para realizar cambios**.**
- **Telnet Session (Heavy):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Remote Login** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá 3.8 una tabla que deberá quedar con las siguientes especificaciones:

Tabla 3.8. Configuración File Print (Heavy)

Inter Command Time-(Seconds)	**Distribution name:** Normal **Mean outcome:** 30 **Variance:** 5
Termianl Traffic (bytes per command)	**Distribution name:** Normal **Mean outcome :** 60 **Variance:** 144
Host Traffic (bytes per command)	**Distribution name :** Normal **Mean outcome :** 25 **Variance:** 25
Symbolic Server Name	**Remote Login Server**
Type of service	**Best Effort (0)**
RSVP Parameter	**None**
Back- End Custom Application	**Not used**

Autores

Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Telnet Session (Light):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Remote Login** que tiene por defecto el valor **Off,** busque **Low Load** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **Video Conferencing (Heavy):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing**

que tiene por defecto el valor **Off,** busque **VCR Quality Video** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**

- **Video Conferencing (Light):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing** que tiene por defecto el valor **Off.** busque **Low Resolution Video** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **light_video:** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Video Conferencing** que tiene por defecto el valor **Off.** Elija nuevamente **edit,** y aparecerá una tabla 3.9 que deberá quedar con las siguientes especificaciones.

Tabla 3.9. Configuración Video Conferencing (excellent effort)

Frame Interrival Time Information	**Incoming Stream Interrival Time (seconds):** **Distribution name:** constant **Mean outcome:** 0.5 **Outcoming Stream Interrival Time (seconds):** **Distribution name:** constant **Mean outcome:** 0.5
Frame Size Information (bytes)	**Incoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 172 **Outcoming Stream Frame Size(bytes)** **Distribution name:** constant **Mean outcome:** 172
Symbolic Destination Name	**Video Destination**
Type of service	**Best Effort(0)**
RSVP Parameter	**None**
Traffic Mix (%)	**All Discrete.**

Autores

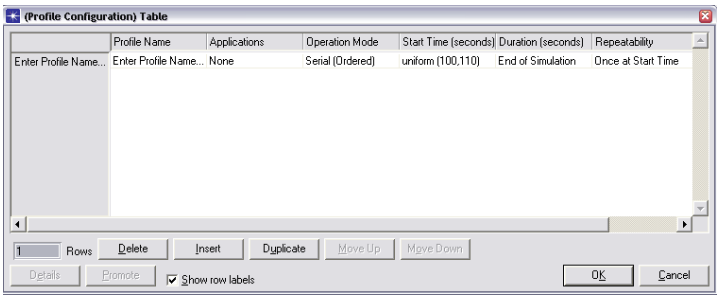
Finalice oprimiendo **OK,** para guardar los cambios**.**

- **Voice over IP Call (PCM Quality):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Voice** que tiene por defecto el valor **Off,** busque **PCM Quality and Silence Suppressed** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**

- **Voice Over IP Call (GSM Quality):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Voice** que tiene por defecto el valor **Off,** busque **GSM Quality Speech** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **Web Browsing (Heavy HTTP 1.1):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Http** que tiene por defecto el valor **Off,** busque **Heavy Browsing** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**
- **Web Browsing (Light HTTP 1.1):** Busque la opción **edit**, de la columna **Description** aparece una ventana y seleccione **Http** que tiene por defecto el valor **Off,** busque **Light Browsing** y asigne este valor. Finalice oprimiendo **OK,** para guardar cambios**.**

3.5 Configuración de los perfiles: Configure el **Profiles**, haga click sobre este icono, seleccione **Edit Attributes**; busque la opción **Profile Configuration,** oprima click sobre **None**, busque **edit,** aparece una tabla como se muestra en la figura 3.8 y agreguele **1 fila (rows)**.

Figura 2.15. Configuración del perfil



Modifique los campos de **Profile Name, Operation Mode y Star Time (seconds)** con los siguientes nombres de la tabla 3.10

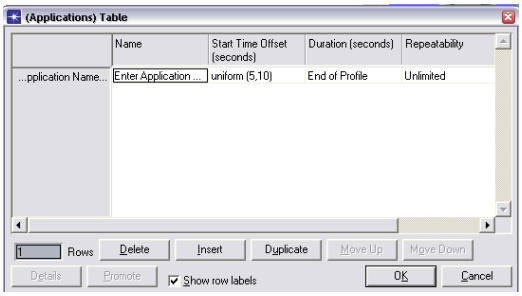
Tabla. Configuración de Perfil de Tráfico

Profile Name	Operation Mode	Star Time (seconds)	Duration (Seconds)	Repeatebility
Video	Serial (Ordered)	**Distribution Name:** constant **Mean outcome:** 60	**End of Simulation**	**Once at Start Time**

Autores

Además en la opción **Applications** de **Video,** que se encuentra en **(Profile Configuration Table)** y esta por defecto en el valor **None,** busque **edit**, aparece una tabla como se muestra en la figura 3.9 y agregue **1 fila (rows).**

Figura 3.9 Aplicación



Modifique lo siguiente como se muestra en la tabla 3.11.

Tabla3.11. Configuración de la aplicación light_video

Name	**Star Time Offset (Seconds)**	**Durations Seconds**	**Repeatability**
light_video	No offset	End to Profile	Unlimited

Autores

En **Applications Table,** oprima **OK** para realizar los cambios.

3.6 Configuración de los Routers y Estaciones: ubíquese en **Foreign_Router_0,** realice click derecho, seleccione **Edit Attributes**; ahí encontrara información de la estación. En la opción **IP,** luego **IPv6 Parameters,** busque **Interface Information** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** que se encuentra en cero (0), edite el número 2.

- Abra la opción **IF0** que tiene por defecto este nombre y cambie el nombre por **IF1** y coloque lo siguiente; **Link local address** en **Default EUI-64,** además despliegue el menú de **Global Address (es)** oprimiendo en el icono (+) y oprima click en **(…)** y busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que se encuentra en **Not Active** busque **edit;**

coloque **2001:200::1,** además **Address type** debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. El **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng.** Además en la opción **Router Advertisement Parameters** que tiene el valor de **Default,** busque **Edit,** aparecerá una tabla 3.12 como se muestra a continuación:

Tabla 3.12. Configuración de los anuncios de Foreign_Router_0

Atributo	Valor
Router Advertisment	Enabled
Router Advertisment Interval (sec)	Distribution name: uniform Minimun outcome: 0.5 Maximum outcome: 1
Current Hop Limit (hops)	32
Advertisment Lifetime (sec)	Half Hour
Advertisment Reachable Time (msec)	Unspecified
Advertisment Prefix List	All
Advertisment Interval (msec)	Auto Calculate

Autores

Neighbor Cache Paramenters, debe encontrarse en **default** y la opción **Subinterface Information,** debe estar en **None.**

- Abra nuevamente la otra opción **IF0** y cambie el nombre por **IF2** y coloque lo siguiente; **Link local address** en **Default EUI-64,** además despliegue el menú de **Global Address (es)** oprimiendo en el icono (+) y oprima click en **(…)** y busque la opción **edit**, donde se abrirá una ventana **(Global Address(es) Table),** allí en la opción **Address** que se encuentra en **Not Active** busque **edit;** coloque **2001:196::2,** además **Address type** debe encontrarse en **Non EUI-64,** oprima **OK** para guardar cambios. El **Routing Protocol(s)** debe tener habilitado el parámetro **RIPng. Router Advetisement Paramenters** y **Neighbor Cache Paramenters**, se deben encontrar con el valor de **Default.** Seguidamente **Subinterface Information,** debe estar en **None.**

En el mismo **Foreign_Router_0**, en la opción **IP,** seguido de **IP Routing Parameters,** se encuentra **Interface information (6 Rows),** despliegue la

opción anterior oprimiendo click en (+), oprima click sobre (…), donde aparecerá una tabla, modifique la dirección **(Address)** de **IF2, IF3, IF4 e IF5**, por **No IP Address**. Finalice oprimiendo click en **OK** para guardar cambios.

Ahora en los mismos atributos de **Foreign_Router_0,** despliegue el menú de opción **Wireless LAN,** encontrara **Wireless LAN Paramenters** y abra este menú, donde encontrara dos parámetros: **BSS Identifier** al cual le asignara el valor **3,** y el parámetro **Data Rate (bps)** el valor de **1 Mbps.**

Los pasos anteriores se repiten para **HA_A, Foreign_Router_1** y **HA_B** modificando lo siguiente;

Configuración HA_A

- **IP→ IPv6 Parameters → Interface Information→ Number of Rows (2),** y modifique lo siguiente como se muestra en la tabla 3.13.

Tabla 3.13. Configuración de HA_A

<table>
<tr><th>Name</th><th>IF1</th><th>IF2</th></tr>
<tr><td>Link Local Address</td><td colspan="2">Default EUI-64</td><td>Default EUI-64</td></tr>
<tr><td>Global Address</td><td colspan="2">2001:193::1</td><td>2001:194::1</td></tr>
<tr><td>Routing Protocol(s)</td><td colspan="2">RIPng</td><td>RIPng</td></tr>
<tr><td>Router Advertisement Paramenters</td><td colspan="2"><table><tr><th>Atributo</th><th>Valor</th></tr><tr><td>Router Advertisment</td><td>Enabled</td></tr><tr><td>Router Advertisment Interval (sec)</td><td>Distribution name: uniform
Minimun outcome: 0.5
Maximum outcome: 1</td></tr><tr><td>Current Hop Limit (hops)</td><td>32</td></tr><tr><td>Advertisment Lifetime (sec)</td><td>Half Hour</td></tr><tr><td>Advertisment Reachable Time (msec)</td><td>Unspecified</td></tr><tr><td>Advertisment Prefix List</td><td>All</td></tr><tr><td>Advertisment Interval (msec)</td><td>Auto Calculate</td></tr></table></td><td>Default</td></tr>
<tr><td>Neighbor Cache Paramenters</td><td colspan="2">Default</td><td>Default</td></tr>
<tr><td>Subinterface information</td><td colspan="2">None</td><td>None</td></tr>
</table>

Autores

En **HA_A**, en la opción **IP →IP Routing Parameters→Interface Information (6 Rows),** despliegue la opción anterior oprimiendo click en (+), oprima click sobre (…), donde aparecerá una tabla, modifique la dirección **(Address)** de **IF2, IF3, IF4 e IF5**, por **No IP Address**. Finalice oprimiendo click en **OK** para guardar cambios.

En **IP→Mobile IP Router Parameters→Mobile IPv6 Paramenters,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** asígnele el valor de **1** y despliegue la opción **Specif,** donde se modifica la siguiente como se muestra en la tabla 3.14

Tabla 3.14. Configuración del HA_A en IPv6

Interface Name	IF1
Interface Type	Home Agent
Home Agent Parmeters	Default

Autores

Finalice oprimiendo click en **OK,** para guardar cambios.

Ahora en los mismos atributos de **HA_A,** despliegue el menú de opción **Wireless LAN,** encontrara **Wireless LAN Paramenters** y abra este menú, donde encontrara dos parámetros: **BSS Identifier** al cual le asignara el valor **0,** y el parámetro **Data Rate (bps)** el valor de **1 Mbps.**

Configuración Foreign_Router_1

- **IP→ IPv6 Parameters → Interface Information→ Number of Rows (2),** y modifique lo siguiente como se muestra en la tabla 3.15

Tabla 3.15. Configuración de Foreign_Router_1

<table>
<tr><th>Name</th><th>IF1</th><th>IF2</th></tr>
<tr><td>Link Local Address</td><td>Default EUI-64</td><td>Default EUI-64</td></tr>
<tr><td>Global Address</td><td>2001:197::1</td><td>2001:198::1</td></tr>
<tr><td>Routing Protocol(s)</td><td>RIPng</td><td>RIPng</td></tr>
<tr><td>Router Advertisement Paramenters</td><td>
<table>
<tr><th>Atributo</th><th>Valor</th></tr>
<tr><td>Router Advertisment</td><td>Enabled</td></tr>
<tr><td>Router Advertisment Interval (sec)</td><td>Distribution name: uniform
Minimun outcome: 0.5
Maximum outcome: 1</td></tr>
<tr><td>Current Hop Limit (hops)</td><td>32</td></tr>
<tr><td>Advertisment Lifetime (sec)</td><td>Half Hour</td></tr>
<tr><td>Advertisment Reachable Time (msec)</td><td>Unspecified</td></tr>
<tr><td>Advertisment Prefix List</td><td>All</td></tr>
<tr><td>Advertisment Interval (msec)</td><td>Auto Calculate</td></tr>
</table>
</td><td>Default</td></tr>
<tr><td>Neighbor Cache Paramenters</td><td>Default</td><td>Default</td></tr>
<tr><td>Subinterface information</td><td>None</td><td>None</td></tr>
</table>

Autores

En **Foreign_Router_1,** en la opción **IP →IP Routing Parameters→Interface Information (6 Rows),** despliegue la opción anterior oprimiendo click en (+), oprima click sobre (…), donde aparecerá una tabla, modifique la dirección **(Address)** de **IF2, IF3, IF4 e IF5**, por **No IP Address**. Finalice oprimiendo click en **OK** para guardar cambios.

Ahora en los mismos atributos de **Foreign_Router_1,** despliegue el menú de opción **Wireless LAN,** encontrara **Wireless LAN Paramenters** y abra este menú, donde encontrara dos parámetros: **BSS Identifier** al cual le asignara el valor **2,** y el parámetro **Data Rate (bps)** el valor de **1 Mbps.**

Configuración HA_B

- **IP→ IPv6 Parameters → Interface Information→ Number of Rows (2),** y modifique lo siguiente como se muestra en la tabla 3.16.

Tabla3.16. Configuración de HA_B

<table>
<tr><th>Name</th><th>IF1</th><th>IF2</th></tr>
<tr><td>Link Local Address</td><td>Default EUI-64</td><td>Default EUI-64</td></tr>
<tr><td>Global Address</td><td>2001:192::1</td><td>2001:195::1</td></tr>
<tr><td>Routing Protocol(s)</td><td>RIPng</td><td>RIPng</td></tr>
<tr><td>Router Advertisement Paramenters</td><td>
<table>
<tr><th>Atributo</th><th>Valor</th></tr>
<tr><td>Router Advertisment</td><td>Enabled</td></tr>
<tr><td>Router Advertisment Interval (sec)</td><td>Distribution name: uniform
Minimun outcome: 0.5
Maximum outcome: 1</td></tr>
<tr><td>Current Hop Limit (hops)</td><td>32</td></tr>
<tr><td>Advertisment Lifetime (sec)</td><td>Half Hour</td></tr>
<tr><td>Advertisment Reachable Time (msec)</td><td>Unspecified</td></tr>
<tr><td>Advertisment Prefix List</td><td>All</td></tr>
<tr><td>Advertisment Interval (msec)</td><td>Auto Calculate</td></tr>
</table>
</td><td>Default</td></tr>
<tr><td>Neighbor Cache Paramenters</td><td>Default</td><td>Default</td></tr>
<tr><td>Subinterface information</td><td>None</td><td>None</td></tr>
</table>

Autores

En **HA_B**, en la opción **IP →IP Routing Parameters→Interface Information (6 Rows),** despliegue la opción anterior oprimiendo click en (+), oprima click sobre (…), donde aparecerá una tabla, modifique la dirección **(Address)** de **IF3, IF4 e IF5**, por **No IP Address**. Finalice oprimiendo click en **OK** para guardar cambios.

En **IP→Mobile IP Router Parameters→Mobile IPv6 Paramenters,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** asígnele el valor de **1** y despliegue la opción **Specif,** donde se modifica lo siguiente como se muestra en la tabla 3.17

Tabla 3.17. Configuración del HA_B en IPv6

Interface Name	IF1
Interface Type	Home Agent
Home Agent Parmeters	Default

Autores

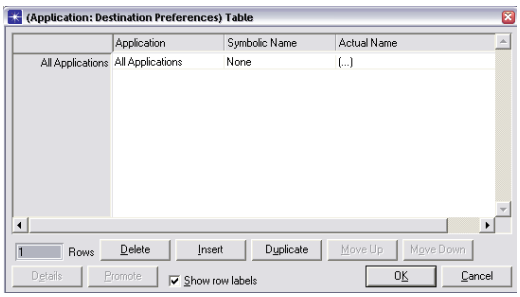
Finalice oprimiendo click en **OK,** para guardar cambios.

Ahora en los mismos atributos de **HA_B,** despliegue el menú de opción **Wireless LAN,** encontrara **Wireless LAN Paramenters** y abra este menú, donde encontrara dos parámetros: **BSS Identifier** al cual le asignara el valor **1,** y el parámetro **Data Rate (bps)** el valor de **1 Mbps.**

Ubíquese en la estación **MN_A,** realice click derecho, seleccione **Edit Attributes**, seleccione **trajectory** que tiene como valor **None** y cámbielo por **mipv6_eight_points_A.**

Despliegue la opción **Applications** luego **Applications: Destination Preferences** que por defecto tiene valor **None,** busque la opción **Edit ,** y aparecerá una tabla como la siguiente en donde deberá agregar **1 fila (rows).**

Figura 3.10. Preferencia de destino



Modifique de la tabla la opcion **Symbolic Name,** que viene con la opción **None** por **Video Destination,** y en **Actual Name** oprima click sobre **(…)** donde aparece una tabla en la cual deberá agregar **1 fila (rows).** En **Name** que tiene por defecto el valor **None,** busqué la opción **Edit**, coloque **mn_client** y en **Selection Weight** coloque el valor de **10**. Finalice oprimiendo **OK,** para guardar cambios.

Ahora se modifica **Application: Suported Profiles** que tiene por defecto el valor **None,** busque la opción **Edit ,** y aparecerá una tabla como la siguiente en donde deberá agregar **1 fila (rows).** Se modificara el **Profile name** que tiene **None** por **Video**, además el **Traffic Type** debe estar en la opción **All discrete** y **Application Delay Tracking** debe estar **Disabled,** finalice oprimiendo **OK** para realizar cambios.

En la opción **IP→ IP Host Parameters →Interface Information,** despliegue todo el menú y debe tener asignado lo siguiente:

- **Address,** oprimiendo click sobre la opción **Auto Assigned**
- **Subnet mask**, oprimiendo click sobre la opción **Auto Assigned**
- **MTU(bytes),** debe estar en **WLAN**

Además en → **IP Host Parameters →Interface Information→ IPv6 Parameters** oprimiendo click sobre el icono (+) se modificara algunos parámetros como:

- **Link Local Address** que se encuentra en la opción **Not Active,** asigne **Default EUI-64. Global Address (es)** despliegue el icono (+), y encontrara la opción **Not Active,** cambie la dirección **(Address)** que se está en **Not Active,** en **Edit** por **2001:193::2**, y **Address Type** debe estar en **Non EUI-64.** Para finalizar oprima click en **OK** guardar cambios.

En la opción **IP→Mobile IP Host Parameters →Mobile IPv6 Paramenters,** despliegue la opción anterior oprimiendo click en (+), modifique lo siguiente como se muestra en la tabla 3.18.

Tabla3.18. Configuración del MN_A en IPv6

Node Type	Mobile Node
Route Optimization	Enabled
Home Agent Address	2001:193::1

Autores

Despliegue el menú de opción **Wireless LAN→Wireless LAN Paramenters** y abra este menú, donde encontrara dos parámetros: **BSS Identifier** al cual le asignara el valor **0,** y el parámetro **Data Rate (bps)** el valor de **1 Mbps.** Busque la opción **Roaming Capacibility** y **habilítelo.**

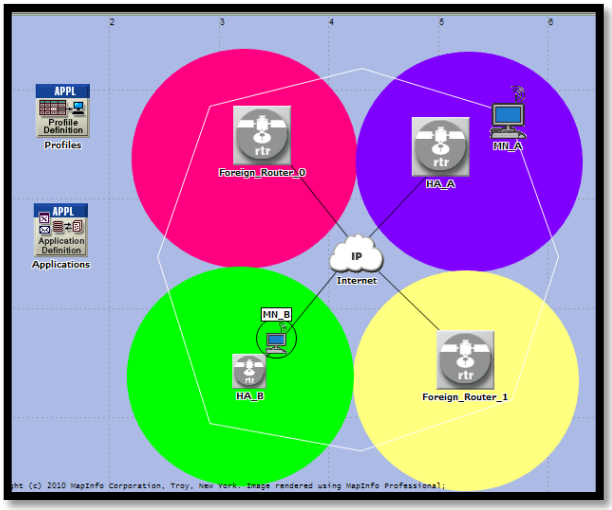
Busque la opción **TCP,** despliegue el menú **TCP Parameters,** ubique y asigne los siguientes valores como se muestra en la tabla 3.19

Tabla 3.19. Parámetros del tiempo de espera para la retransmisión MN_A

Initial RTO (sec)	20
Minimum RTO (sec)	10
Maximum RTO (sec)	120

Autores

Finalice oprimiendo click en **OK,** en la tabla de atributos. Saldrá un octágono que indicara la ruta de la estación organice, los elementos similar a esta forma.



Se realice los pasos anteriore, para configurar la estación de **MN_B,** modificando los siguientes valores, como se muestran en la tabla 3.20:

- **Edit attributes→ trajectory → mipv6_eight_point_B-**
- **Applications → Application: Destination Preferences,** Agregar 1 fila **(rows).**

Tabla3.20. Preferencias de Destino MN_B

Application	**Symbolic Name**	**Actual Name (agregar 1 rows)**	
All Aplication	Video Destination	**Name:** serv	**Selection Weigth:** 10

Autores

- **Applications → Application: Supported Services** debe estar en **All.**
- **IP→ IP Host Parameters → Interface Information**, debe tener asignado la siguiente información como se muestra en la tabla 3.21:

Tabla 3.21. Interfaz de Información del MN_B

Address	Auto Assigned
Subnet Mask	Auto Assigned
MTU(bytes)	WLAN

Autores

- **IP→ IP Host Parameters→ Interface Information→ IPv6 Parameters**: como se muestra en la table 3.22

Tabla 3.22. Interfaz de Información en IPv6 del MN_B

Link local address	Default EUI-64
Global address (es) **Address:** **Address Type:**	 2001:192:27 Non EUI-64

Autores

En la opción **IP→Mobile IP Host Parameters →Mobile IPv6 Paramenters,** despliegue la opción anterior oprimiendo click en (+), modifique lo siguiente como se muestra en la tabla 3.23

Tabla 3.23. Configuración del MN_B en IPv6

Node Type	Mobile Node
Route Optimization	Enabled
Home Agent Address	2001:192::1

Autores

En la opción **Wireless LAN→Wireless LAN Paramenters** y abra este menú, donde encontrara dos parámetros: **BSS Identifier** al cual le asignara el valor **1,** y el parámetro **Data Rate (bps)** el valor de **1 Mbps.** . Busque la opción **Roaming Capacibility** y **habilítelo.**

Busque la opción **TCP,** despliegue el menú **TCP Parameters,** ubique y asigne los siguientes valores como se muestra en la tabla 3.24.

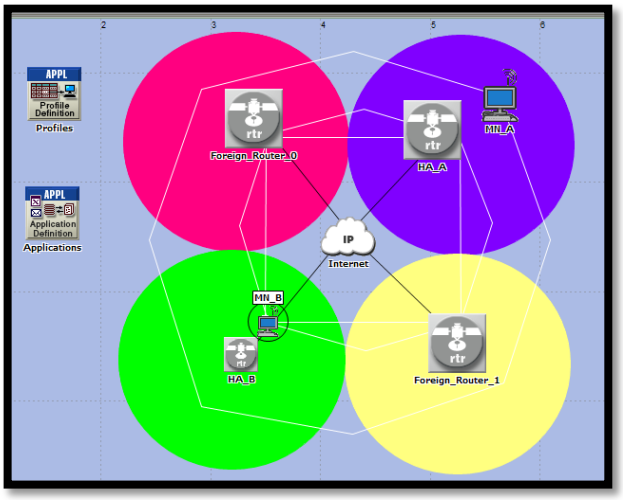
Tabla 3.24. Parámetros del tiempo de espera para la retransmisión MN_B

Initial RTO (sec)	20
Minimum RTO (sec)	10
Maximum RTO (sec)	120

Autores

Finalice oprimiendo click en **OK,** en la tabla de atributos. Saldrá un octágono que indicara la ruta de la estación. Organice los elementos similares a la figura 3.10. Para cambiar el color de la trayectoria, realice click sobre el elemento **MN_B**, elija **Edit Attributes,** en la parte inferior seleccione la pestana **Advanced,** seleccione **color** y cámbielo a su gusto.

Figura 3.10. Escenario MIPv6 con trayectorias



3.7 Configuración de la nube Internet: Ubíquese en el elemento de **INTERNET,** realice click derecho, seleccione **Edit Atrributes**; Ingrese a la opción **IP,** seguido de **IPv6 Parameters,** busque **Interface Information,** despliegue la opción anterior oprimiendo click en (+) y en **Number of Rows** agregue 5 filas **(5 Rows)** y modifique la siguiente información como se muestra en la tabla 3.25.

Tabla 3.25. Configuración Nube Internet

Name	**IF0**	**IF1**	**IF2**	**IF4**	**IF3**
Link Local Address	Default EUI-64	Default EUI-64	Default EUI-64	Default EUI-64	Default EUI-64
Global Address (es) **Address** **Prefix Length (bits)** **Address Type**	 2001:194::2 64 Non EUI-64	 2001:195::2 Non EUI-64	 2001:196::1 Non EUI-64	 2001:198::5 Non EUI-64	 2001:199::5 Non EUI-64
Routing Protocol(s)	RIPng	RIPng	RIPng	RIPng	RIPng
Router Advetisement	default	default	default	default	default
Neighbor Cache Paramenters	default	default	default	default	default
Subinterface information	None	None	None	None	None

Autores

En la nube **Internet** busque la opción **IP →IP Routing Parameters→Interface Information (8 Rows),** despliegue la opción anterior oprimiendo click en (+), oprima click sobre (…), donde aparecerá una tabla, modifique la dirección **(Address)** de **IF2, IF3, IF4, IF5, IF6 e IF7** por **No IP Address**. Finalice oprimiendo click en **OK** para guardar cambios.

Despliegue el menú de la Opción **Packet Lantency (secs)** que debe estar en **0.1,** finalice oprimiendo click sobre **OK** en la tabla de atributos, para guardar cambios.

3.8 Selección de resultados: En el escenario principal, realice click derecho, seleccione la opción **Choose individual DES statistics,** seleccione lo siguiente como se muestra en la tabla 3.26.

Tabla3.26. Selección de resultados

Global Statistics	Node Statistics
• **Mobile IPv6**	• **Mobile IPv6**
✓ Route Optimization Overhead (bits/sec	✓ Active Access Point
✓ Route Optimization Traffic Received (bits/sec)	✓ Binding Cache Table Size
✓ Route Optimization Traffic Received (pkts/sec)	✓ Binding Update List Size
✓ Route Optimization Traffic sent (bits/sec)	• **Video Called Party**
✓ Route Optimization Traffic sent (pkts/sec)	✓ Packet Delay Variation
✓ Tunneled Traffic Overhead (bits/sec)	✓ Traffic Received (bytes/sec)
✓ Tunneled Traffic Received (bits/sec)	✓ Traffic Sent (bytes/sec)
✓ Tunneled Traffic Received (pkts/sec)	• **Video Calling Party**
✓ Tunneled Traffic sent (bits/sec)	✓ Packet Delay Variation
✓ Tunneled Traffic sent (pkts/sec)	✓ Traffic Received (bytes/sec)
• **Video Conferencing**	✓ Traffic Sent (bytes/sec)
✓ packet End - to- End (sec)	

Autores

3.9 Duplicar escenario; Luego de anterior se duplica el escenario en el menú **Scenarios,** en la opción **Duplicate Scenario,** allí saldrá una ventana, coloque como Scenario name: **Disabled,** Oprima **OK** para finalizar, se duplicara el escenario, si quiere regresar al escenario anterior que se llama **enabled,** regrese al menú **Scenarios,** diríjase **Switch To Scenario,** allí aparecerán los dos escenarios que se crearon.

En este escenario lo único se modifica es lo siguiente:

Ubíquese en la estación **MN_A,** realice click derecho, seleccione **Edit Attributes** En la opción **IP→Mobile IP Host Parameters →Mobile IPv6 Paramenters,** despliegue la opción anterior oprimiendo click en (+), modifique lo siguiente como se muestra en la tabla 3.27.

Tabla3.27. Configuración del MN_A en IPv6 deshabilitado

Node Type	Mobile Node
Route Optimization	Disabled
Home Agent Address	2001:193::1

Autores

Ubíquese en la estación **MN_B,** realice click derecho, seleccione **Edit Attributes** En la opción **IP→Mobile IP Host Parameters →Mobile IPv6 Paramenters,** despliegue la opción anterior oprimiendo click en (+), modifique lo siguiente como se muestra en la tabla 3.28.

Tabla 3.28. Configuración del MN_B en IPv6 deshabilitado

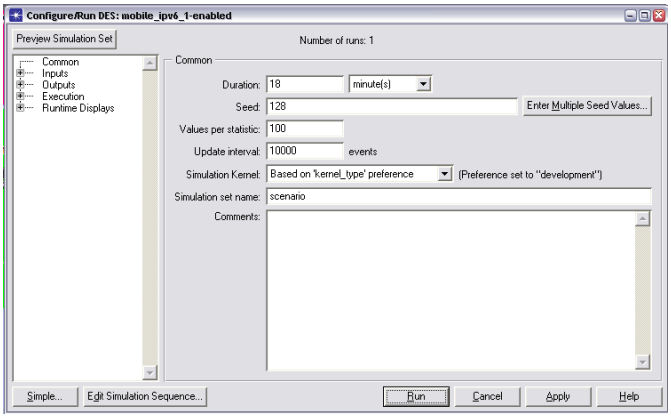
Node Type	Mobile Node
Route Optimization	Disabled
Home Agent Address	2001:192::1

Autores

3.10 Realización de simulación: Para llevar a cabo la simulación, realice los siguientes pasos;

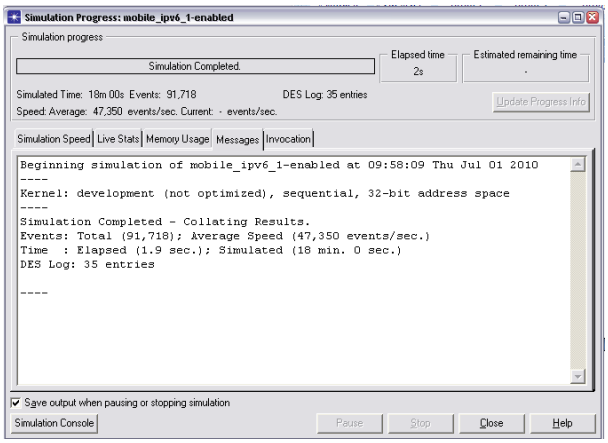
- En la barra de herramientas se encuentra el icono RUN  donde aparece una ventana mostrando la duración de la simulación como se muestra en la figura 3.12; esta duración se puede modificar para ver mayores intervalos de tiempo. Asigne los siguiente; Duration 18 minutos, seed 128, values per statistics 100, Update interval 100000

Figura 3.12. Parámetros para la simulación



Después de configurar estos parámetros, haga click en **RUN** y se observara como se muestra en la figura 3.13

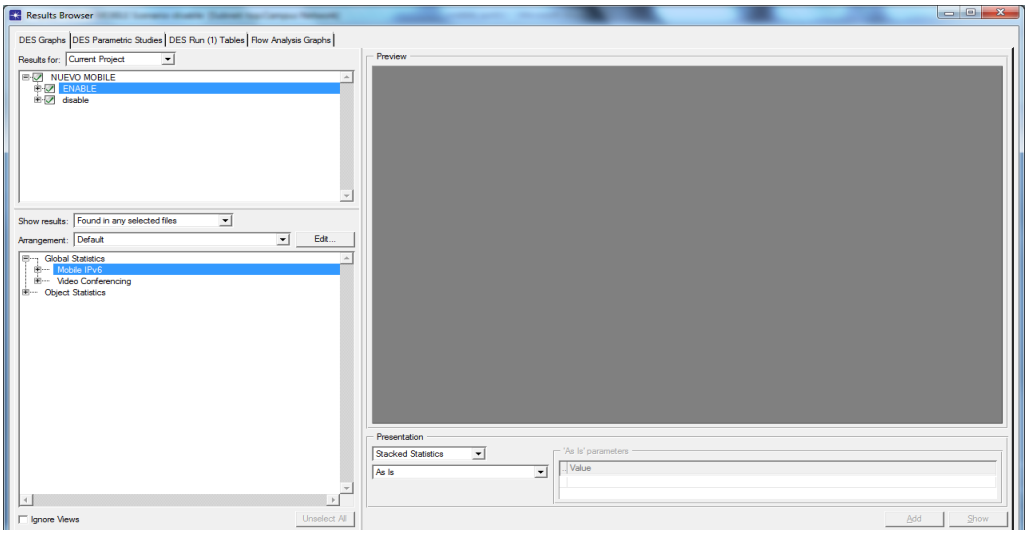
Figura 3.13 Detección de errores



De esta manera al terminar el proceso de detección de errores se cierra la ventana en el botón **close**.

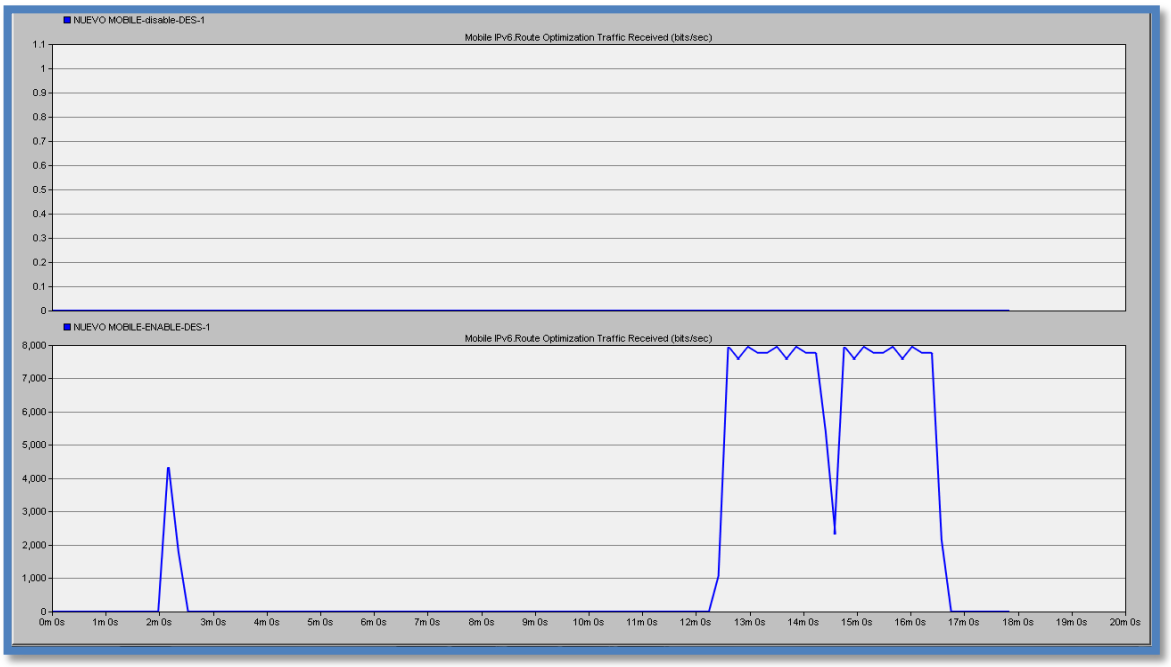
3.11 Resultados: Para revisar la tabla de resultados se ingresa al menú **Flow Analysis,** posteriormente se buscara **Results**, se dará click en **View Results** y aparece la siguiente ventana (**Result Browser)**, donde se debe ingresar a la pestana **DES Graphs**. En la opción **Result For** debe estar en **Current Project.** Seleccionar **enabled y disabled.** Como se muestra en la figura 3.14

Figura 3.14. Visualización de Resultados

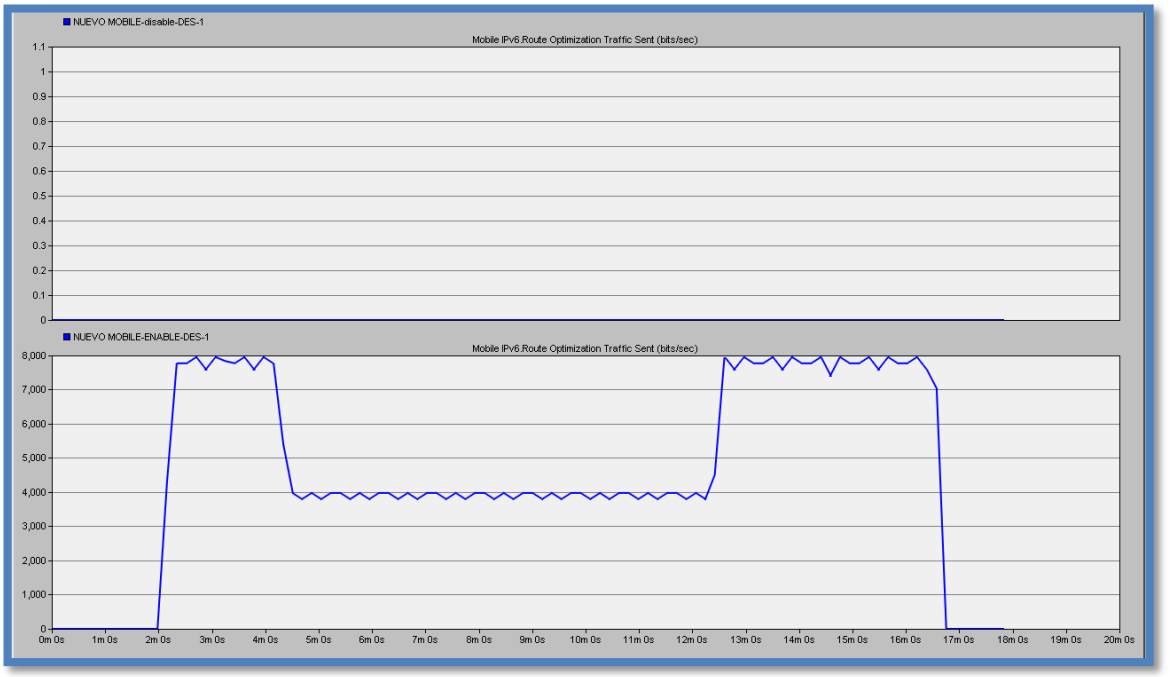


Algunos de los Resultados esperados. GRAFICOS DE MOBILE IPV6

Trafico recibido de Ruta optimizada en el escenario habilitado y deshabilitado

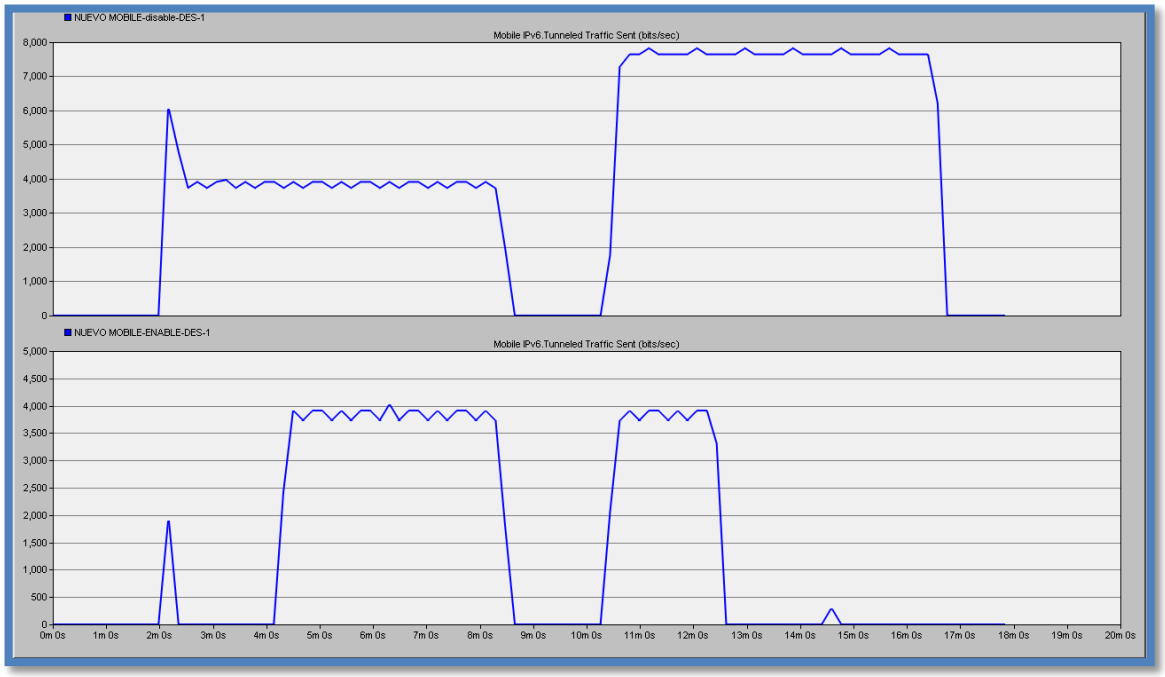


Trafico enviado de Ruta optimizada en el escenario habilitado y deshabilitado.

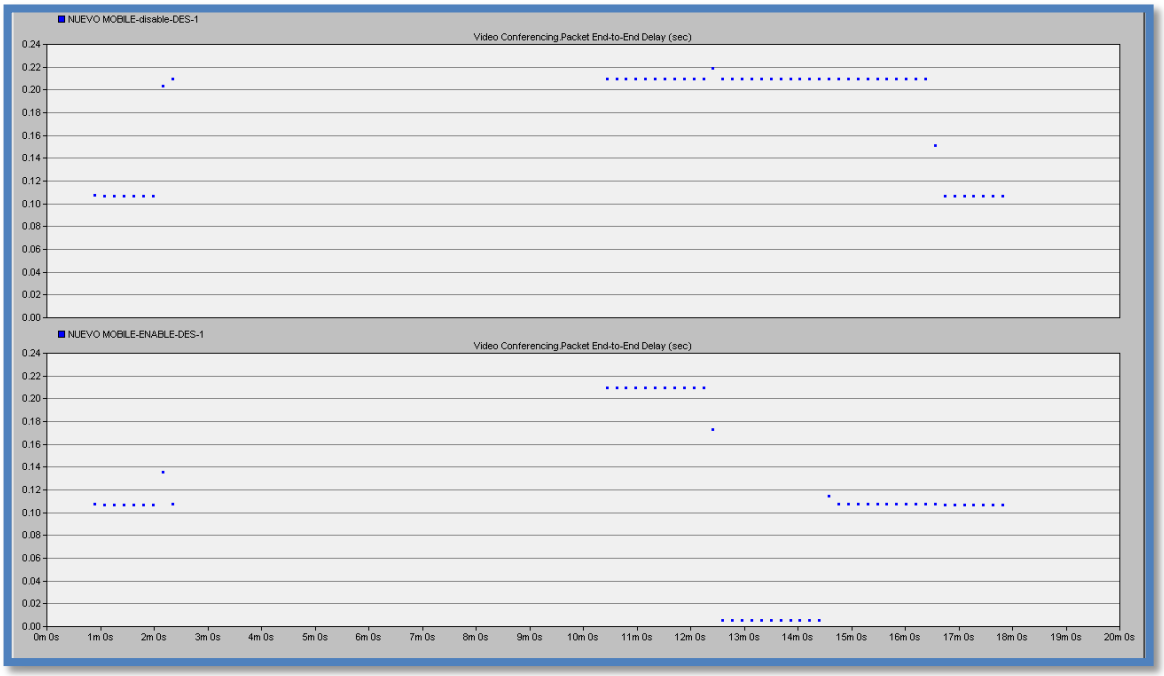


Trafico recibido en el TUNEL del escenario habilitado y deshabilitado.

Trafico enviado en el TUNEL del escenario habilitado y deshabilitado.



Resultado de video conferencing de End to End



Tarea:

Cambie las velocidades de las trayectorias, para observar que pasa con las gráficas, para realizar este proceso, realice click derecho sobre cada trayectoria y escoja la opción **edit trajectory,** modifique la opción **Ground Speed.**