

WIRELESS SOBRE OPNET

WOLFGANG A. HOLLMAN MUNERA

DANIEL SANJUAN ENCISO

UNIVERSIDAD TECNOLOGICA DE BOLIVAR

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

AREA DE TELECOMUNICACIONES

CARTAGENA DE INDIAS

2006

WIRELESS SOBRE OPNET

WOLFGANG A. HOLLMAN MUNERA	0204024
DANIEL SANJUAN ENCISO	0204056

Monografía para optar al título de
INGENIERO ELECTRONICO

Director

JORGE E. DUQUE PARDO

Ingeniero Electricista

Msc. Ingeniería Electrónica

UNIVERSIDAD TECNOLOGICA DE BOLIVAR
FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA
AREA DE TELECOMUNICACIONES
CARTAGENA DE INDIAS
2006

RESUMEN

La tendencia a la movilidad y la ubicuidad hacen cada vez más utilizados los sistemas inalámbricos, y el objetivo es ir evitando los cables en todo tipo de comunicación, no solo en el campo informático sino en televisión, telefonía, Seguridad, Domótica, etc.

Referido a las telecomunicaciones, se aplica el término **inalámbrico** (inglés *wireless*) al tipo de comunicación en la que no se utiliza un medio de propagación físico, sino se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión.

Un fenómeno social que ha adquirido gran importancia en todo el mundo como consecuencia del uso de la tecnología inalámbrica son las comunidades wireless que buscan la difusión de redes alternativas a las comerciales. En general, la tecnología inalámbrica utiliza ondas de radiofrecuencia de baja potencia y una banda específica, de uso libre para transmitir, entre dispositivos. Estas condiciones de libertad de utilización, sin necesidad de licencia, han propiciado que el número de equipos, especialmente computadoras, que utilizan las ondas para conectarse, a través de redes inalámbricas haya crecido notablemente.

En realidad las redes *wireless* presentan un grupo de ventajas sobre las redes cableadas:

Movilidad: Los usuarios se mueven, pero los datos comúnmente se encuentran centralizados, permitiendo a estos usuarios el acceso a la información mientras se encuentran en movimiento. La oportunidad de acceder a la información desde cualquier punto sin necesidad de la conexión física al puerto permite un gran ahorro de tiempo y productividad, lo que hace de la comunicación inalámbrica pueda ser diseñada bajo conceptos de necesidad de los usuarios.

Facilidad y Rápido Despliegue: Muchas áreas son muy difíciles de cablear para las tradicionales LAN (*Red de área local*) cableadas. La creación de nuevas LANs en algunos sitios se dificulta ya sea por su antigüedad, o por las leyes que rigen la manipulación de estos sitios; sin embargo, en modernas construcciones la instalación de una LAN cableada puede llegar a ser costosa y el consumo del tiempo sería mayor a si se hiciera con tecnología *Wireless*.

Flexibilidad: Sin cables no existe el recableado. Las redes inalámbricas permiten a los usuarios formar redes en cualquier lugar y de cualquier forma: ya sea pequeños grupos de trabajo u oficinas. La expansión de la red en *wireless* es fácil debido a que el acceso a esta se encuentra en todas partes, no hay cables que ponchar, conectar, simplemente es encontrar un punto de acceso a la red y en un momento estaremos trabajando. Flexibilidad por lo tanto, es el punto de venta de mayor relevancia en el mercado, ya que este es utilizado por: hoteles, aeropuertos, cafés, librerías, entre otros.

Costo: En algunos casos, los costos pueden ser reducidos usando tecnología inalámbrica. Por ejemplo, algunos de los equipos inalámbricos pueden ser usados para crear puentes (*bridging*) entre dos edificios. Colocar un puente inalámbrico requiere una inversión inicial considerable en puntos de acceso, equipos e interfaces inalámbricas. Sin embargo, después de esta inversión inicial, simplemente se requiere de un pequeño costo de operación. A medida

que pasa el tiempo, nos daremos cuenta que un puente inalámbrico es mucho menos costoso que contratar un servicio de conexión a una compañía de telecomunicación.

Aunque los sistemas de redes inalámbricos pueden parecer perfectos, realmente no los son, y presentan una serie de inconvenientes que presentaremos a continuación:

Calidad de Servicio: Las redes inalámbricas ofrecen una peor calidad de servicio que las redes cableadas. Estamos hablando de velocidades que no superan habitualmente los 100 Mbps, frente a los 10Gbps que puede alcanzar una red normal y corriente. Por otra parte hay que tener en cuenta también la tasa de error debida a las interferencias. Esta se puede situar alrededor de $1E-4$ frente a las $1E-10$ de las redes cableadas. Esto significa que has 6 órdenes de magnitud de diferencia y eso es mucho. Estamos hablando de 1bit erróneo cada 10.000 bits o lo que es lo mismo, aproximadamente de cada Megabit transmitido, 1 Kbit será erróneo. Esto puede llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad

Dependencia fabricantes: Como la estandarización está siendo bastante lenta, ciertos fabricantes han sacado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo y por lo tanto estando atado a ese fabricante. Esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema como para la recuperación ante posibles fallos. Cualquier empresa o particular que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, punto de enlace, etc.

Restricciones: Estas redes operan en un trozo del espectro radioeléctrico. Éste está muy saturado hoy día y las redes deben amoldarse a las reglas que existan dentro de cada país. Concretamente en España, así como en Francia y en Japón, existen limitaciones en el ancho de banda a utilizar por parte de ciertos estándares.

Seguridad: Por una parte seguridad e integridad de la información que se transmite. Este campo está bastante criticado en casi todos los estándares actuales, que, según dicen no se deben utilizar en entornos críticos cuyos en los cuales un “robo” de datos pueda ser peligroso. Por otra parte este tipo de comunicación podría interferir con otras redes de comunicación (policía, bomberos, hospitales, etc.) y esto hay que tenerlo en cuenta en el diseño.

Teniendo en cuenta el avance que existe en software de informática podemos actualmente probar la aplicabilidad e importancia (*ventajas y desventajas*) de las comunicaciones inalámbricas a partir de simuladores de red (OPNET).

OPNET es un simulador que permite modelar y verificar el comportamiento de una red bajo las condiciones de carga que se especifiquen.

Opnet resulta de mucha importancia, ya que, las tecnologías *Wireless* se han ido incorporando en entornos nunca antes pensados, lo que conlleva a realizar muchos mas estudios para su viabilidad y aplicación en nuevos escenarios a partir del uso adecuado del software mencionado

TABLA DE CONTENIDO

INTRODUCCION	9
1. Capitulo 1. Introducción a las redes inalámbricas.....	10
1.1 QUE ES WIRELESS?	10
1.2 MODOS DE OPERACIÓN DE SISTEMAS INALÁMBRICOS	10
1.2.1 Punto a punto.....	10
1.2.2 Punto de Acceso / Cliente.....	11
1.2.3 Sistema de distribución Inalámbrico (WDS).....	12
1.3 COMPONENTES DE UNA WLAN	13
1.4 FABRICANTES	13
2 Capitulo 2. OPNET.....	14
2.1 QUE ES OPNET?	14
2.2 FASES PARA LA REALIZACION DE UNA SIMULACION EN OPNET ..	14
2.3 COMPONENTES DE OPNET IT.....	15
2.3.1 Editor de Proyecto (Project Editor):.....	15
2.3.2 Botones de herramientas:.....	17
3 Capitulo 3. WIRELESS SOBRE OPNET.....	18
3.1 Wlan simple:	18
3.2 Wlan simple con Fragmentación:	18
3.3 Wlan RTC/CTS:	18
3.4 Wlan con punto de acceso:.....	19
3.5 Wlan Routed:	19
3.6 Wlan Switched:	19
3.7 Wlan PCF (Point Coordination Function):	19
4 Capitulo 4. Conceptos importantes a tener en cuenta	20
4.1.1 Frequency hopping o espectro ensanchado por salto de frecuencia..	20
4.1.2 Media Access Delay	20
4.1.3 Problema del terminal oculto.	21
4.1.4 Fragmentation Threshold.	21
4.1.5 RTS / CTS. Request To Send, Clear To Send	22
4.1.6 Ethernet.....	23
4.1.7 Internet	25
4.1.8 CSMA/CD.....	26
4.1.9 CSMA/CA.....	28
4.1.10 Serial Line Internet Protocol (SLIP).	28
4.1.11 Distributed Coordination Function (DCF).....	29
4.1.12 Point Coordination Function (PCF).....	30
4.1.13 SWITCH.	31
4.1.14 ROUTER.	32
5 Capitulo 5. PRACTICAS DE WIRELESS SOBRE OPNET	33
5.1 WLAN SIMPLE	33
5.1.1 Análisis de resultados	55
5.2 WLAN SIMPLE CON FRAGMENTACION (FRAGMENTATION	
THRESHOLD)	57
5.2.1 Análisis de resultados.	60

5.3	WLAN RTS / CTS (Request to send / Clear to send).....	61
5.3.1	Análisis de resultados	67
5.4	WLAN CON PUNTO DE ACCESO.....	71
5.4.1	Análisis de resultados	86
5.5	WLAN SWITCHED y ROUTED.....	89
5.5.1	Análisis de resultados	96
5.6	WLAN PCF	98
5.6.1	Análisis de resultados.....	101
6	CONCLUSIONES	103
7	GLOSARIO	104
8	ABREVIATURAS Y ACRONIMOS	107
9	BIBLIOGRAFIA.....	108

INTRODUCCION

A través de los últimos años, el mundo ha pasado de ser estático a presentar un gran incremento en la movilidad de la información. Como resultado, las formas tradicionales de redes en el mundo han probado ser inadecuadas para los nuevos retos propuestos por el nuevo estilo de vida de la colectividad en la actualidad. Si los usuarios estuvieran obligados a estar conectados a una red cableada, entonces su movilidad estaría dramáticamente reducida. La conectividad inalámbrica (Wireless), sin embargo, no posee dicha restricción y permite al usuario mucha mas movilidad.

A lo largo de este trabajo, se intentara lograr que las personas tengan una herramienta para el fácil entendimiento de los sistemas de comunicación Wireless bajo la propuesta del simulador de red: OPNET.

1. Capitulo 1. Introducción a las redes inalámbricas.

1.1 QUE ES WIRELESS?

Como se menciona anteriormente, *Wireless* es el tipo de comunicación en la que no se utiliza un medio de propagación físico, sino se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión.

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio (RF) o Luz Infrarroja (IR), actualmente está siendo ampliamente investigada. Las Redes Inalámbricas (*WLANs*) facilitan la operación en lugares donde la computadora o cualquier otro equipo receptor no pueden permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos. Pero la realidad es que esta tecnología está todavía en desarrollo y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

1.2 MODOS DE OPERACIÓN DE SISTEMAS INALÁMBRICOS

1.2.1 Punto a punto

Es el modo de operación más simple de una red inalámbrica, actuando como una red punto a punto entre un conjunto de equipos con adaptadores wireless. No existen Puntos de Acceso ni ningún tipo de equipo que dé soporte a la red en sí. En este modo de operación, la información viaja directamente entre el emisor y receptor sin pasar por ningún otro equipo.

Este es el modo más fácil, rápido y barato de establecer una red inalámbrica, pero presenta la enorme desventaja de que los equipos deben estar dentro del área de cobertura de los demás para comunicarse con ellos, por lo que sólo es aconsejable para redes con pocos equipos y próximos entre sí. Además, no existe un punto de interconexión con la red cableada, si ésta existiera, a no ser que alguno de los equipos actuara como router.

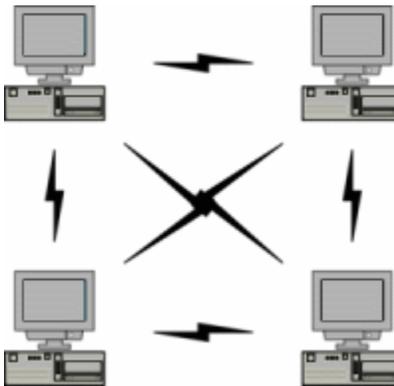


Figura1. Modo Ad-Hoc o Independiente

1.2.2 Punto de Acceso / Cliente

En este modo, cada cliente wireless envía su información a un Punto de Acceso, que la hace llegar al destino adecuado.

La presencia de los Puntos de Acceso eleva el coste de inversión necesario para instalar una red wireless, pero ofrece numerosos beneficios gracias a sus capacidades.

Los Puntos de Acceso permiten aumentar la cobertura de la red wireless, dado que los equipos clientes se comunican con él y no directamente entre sí, y por su condición de equipos fijos ubicados en zonas estratégicas y con antenas de más calidad, ofrecen una mayor cobertura y mejor fiabilidad del enlace.

Los Puntos de acceso actúan normalmente como bridge entre la red cableada y la red inalámbrica, lo que permite el acceso de los clientes wireless a los servicios de la red, aunque también pueden ofrecer servicios más avanzados, como servidores DHCP, así como la posibilidad del empleo de herramientas de seguridad y control de acceso a la red wireless.

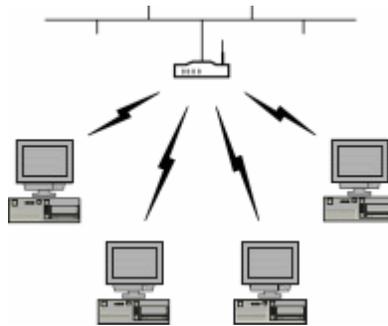


Figura 2. Modo Punto de Acceso

1.2.3 Sistema de distribución Inalámbrico (WDS)

Existe la posibilidad de instalar varios Puntos de Acceso que actúen como repetidores para cubrir áreas mayores permitiendo el roaming de usuarios entre ellos.

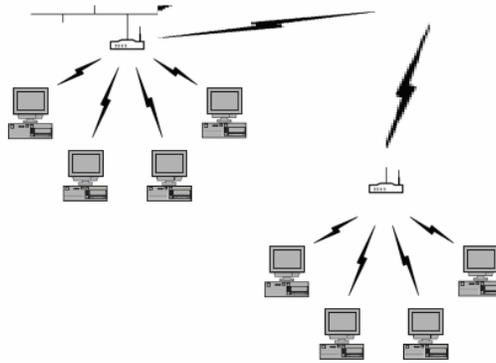


Figura 3. Modo Punto de Acceso Repetidor (WDS)

1.3 COMPONENTES DE UNA WLAN

- Puntos de Acceso
- Dispositivos de captura inalámbricos
- Wlan routers

1.4 FABRICANTES

Entre los principales productores de componentes para la conexión de redes inalámbricas (*WLANs*) se encuentran:

- 3com
- Cisco
- D-link

2 Capitulo 2. OPNET.

2.1 QUE ES OPNET?

En el campo de las redes de telecomunicaciones se ha experimentado un crecimiento exponencial a nivel mundial, esto ha dado lugar a la necesidad de su sofisticación. Por ello se prioriza disponer de un simulador de red que ofrezca herramientas potentes con el objetivo de diseñar modelos, simular datos y analizar las redes. OPNET es un lenguaje de simulación orientado a las comunicaciones. Actualmente es utilizado por grandes empresas de telecomunicaciones, por ejemplo para el desarrollo de proyectos gubernamentales y logísticos.

OPNET proporciona librerías y gracias a ellas se consigue la formación de redes de comunicaciones y se facilita el estudio del desarrollo de los modelos mediante la conexión de diferentes tipos de nodos, utilizando diferentes tipos de enlaces, etc.

2.2 FASES PARA LA REALIZACION DE UNA SIMULACION EN OPNET

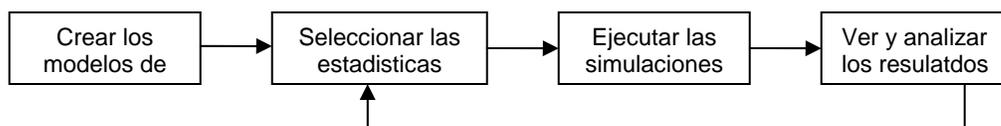


Figura 4. Fases de simulación

Como se puede observar en el esquema superior, la especificación o creación del modelo consiste en desarrollar la representación del sistema a estudiar, con sus respectivas aplicaciones si estas existen. Para esta fase, disponemos de modelos ya realizados en OPNET y de editores para crear modelos propios.

Una vez determinado el modelo, pasamos a especificar las estadísticas a simular, para luego realizar el respectivo análisis y así validar las especificaciones planteadas. En el caso de que estos resultados no fuesen los deseados, se tendría que hacer una re-especificación (nueva selección de estadísticas) donde se modificarían los aspectos erróneos del modelo simulado.

2.3 COMPONENTES DE OPNET IT

A continuación explicaremos las diferentes partes de que consta el OPNET IT, y cuales vamos a utilizar. Los editores incluidos proporcionan las herramientas necesarias para la creación de topologías de red. Cada editor se encarga de una actividad distinta, lo cual se explicara seguidamente.

2.3.1 Editor de Proyecto (Project Editor): El Project editor es el principal escenario de la simulación de la red. Es usado para crear un modelo de red utilizando unos ya existentes que podemos encontrar en la librería estándar, recolectar estadísticas sobre la red, comenzar la simulación y observar resultados.

Este editor contiene tres tipos básicos de objetos: subredes, nodos y enlaces. Las paletas (accesibles mediante un icono en la parte superior izquierda del editor) ordenan los objetos disponibles por categorías. Por ejemplo, en la paleta WLAN, se encuentran los nodos y enlaces mas utilizados para el diseño de este tipo de red.

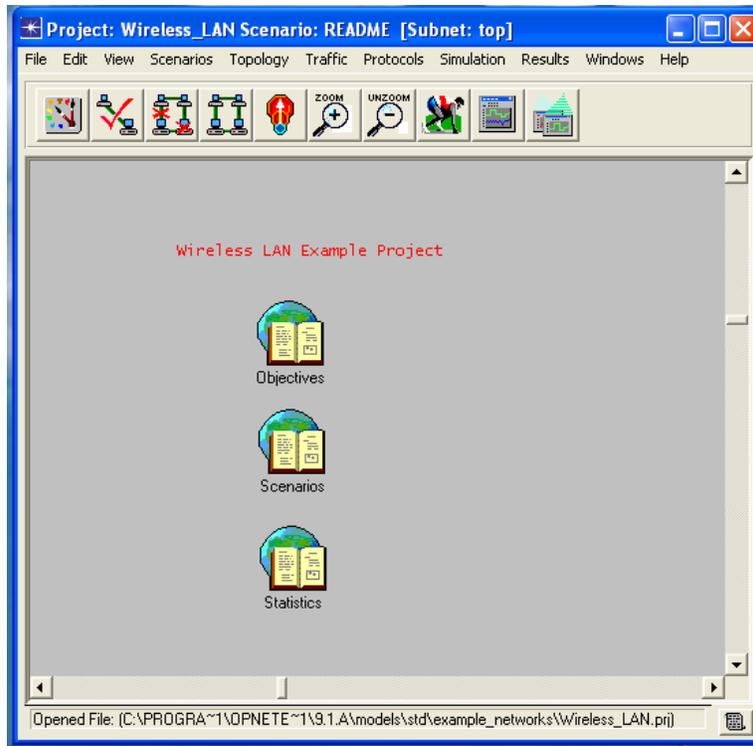


Figura 5. Área de trabajo

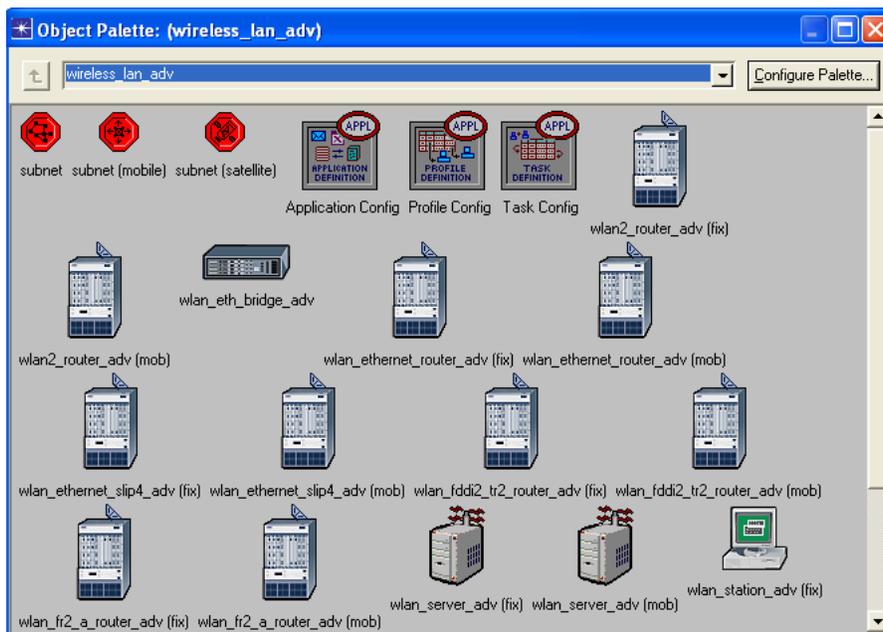


Figura 6. Paleta de objetos

2.3.2 Botones de herramientas: *Las opciones mas habituales del menú pueden ser activadas por medio de estos botones:*



Figura 7. Botones de herramientas.

1. Paleta de objetos
2. Consistencia de un enlace
3. Objetos que no han sido seleccionados
4. Recuperar objetos seleccionados
5. Volver a la subred superior
6. Zoom
7. Reestablecer
8. Configurar un evento discreto de simulación
9. Ver resultados de simulación
10. Esconder o ver todos los gráficos.

3 Capitulo 3. WIRELESS SOBRE OPNET.

Este capítulo prioriza en utilizar el simulador de red previamente mencionado (OPNET IT GURU ACADEMIC EDITION) para que con sus diversas herramientas se puedan diseñar modelos, simular datos y analizar las redes, y así comprender de manera eficiente los diversos conceptos de las tecnologías inalámbricas en sus diferentes escenarios: *wlan simple*, *wlan simple con fragmentación*, *wlan simple con protocolo RTC/CTS*, *wlan con punto de acceso*, *wlan routed network*, *wlan switched network* y por último *wlan PCF*.

3.1 *Wlan simple*: En este escenario se demostrara el comportamiento básico de un modelo de red wireless, en el cual se usara un alto grado de transmisión de datos para la verificación de “conexión física”, es decir, se verificara la operatividad de las capas mas bajas del modelo de comunicaciones. Este escenario también puede ser llamado peer to peer (punto a punto), ya que ambas estaciones se comunican directamente una con otra.

3.2 *Wlan simple con Fragmentación*: Este escenario consiste básicamente en la configuración de una red “Wlan simple”, solo que en este modelo ambas estaciones que conforman la red tendrán la opción de fragmentación habilitada. La opción de fragmentación habilitada en cada una de las estaciones, permitirá una menor tasa del *BER (BIT ERROR RATE)*, entonces lo que determinara esta opción será el tamaño de cada una de las fragmentaciones que se le efectuara al paquete original.

3.3 *Wlan RTC/CTS*: La configuración básica de este escenario consta de dos o mas estaciones inalámbricas, pero con parámetros de intercambio RTC/CTS (Request to send / Clear to send) activados antes de la transmisión de datos.

3.4 Wlan con punto de acceso: Este escenario consiste en la interconexión de una red inalámbrica y una red cableada mediante el backbone de Internet.

3.5 Wlan Routed: Este escenario consiste en una serie de redes locales inalámbricas independientes (Wlan's). Estas redes inalámbricas son conectadas a través de un sistema de distribución cableado. Todas las estaciones en el área seleccionaran el servidor destino por medio de un *wlan_router*.

3.6 Wlan Switched: Este escenario consiste en una serie de redes locales inalámbricas independientes (Wlan's). Estas redes inalámbricas son conectadas a través de un sistema de distribución cableado. Todas las estaciones en el área seleccionaran el servidor destino por medio de un *wlan_switch*.

3.7 Wlan PCF (Point Coordination Function): Este escenario es una demostración del modo de acceso PCF en Wlan's. Básicamente, la infraestructura de red que utiliza este escenario es que cada una de las estaciones de trabajo se comunicaran con las demás a través de un punto de acceso (punto de acceso).

4 Capitulo 4. Conceptos importantes a tener en cuenta

Tanto en los estándares como en este documento se hace extensivo uso de ciertos conceptos, se incluyen aquí las definiciones para mayor provecho del lector. Son de obligado conocimiento para poder entender el resto del documento.

4.1.1 *Frequency hopping o espectro ensanchado por salto de*

frecuencia es una técnica de modulación en espectro ensanchado (*Spread Spectrum*) en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor. Los receptores no autorizados escucharán una señal ininteligible. Si se intentara interceptar la señal, sólo se conseguiría para unos pocos bits. En pocas palabras *Frequency Hopping* es un método para transmitir señales cambiando rápidamente la portadora entre muchas frecuencias, utilizando una secuencia pseudo aleatoria conocida solamente por el transmisor y el receptor.

4.1.2 *Media Access Delay* como su mismo nombre lo indica es el tiempo que tarda el nodo en acceder al medio, es la suma de todos los intentos y retrasos de paquetes de datos recibidos por la capa MAC de una capa mayor. Para cada paquete el retraso es obtenido cuando el paquete es enviado a la capa física por primera vez.

4.1.3 Problema del terminal oculto. En redes de computadoras el problema del terminal oculto ocurre cuando un nodo es visible por un equipo inalámbrico, pero no es visible por los otros nodos que se comunican con dicho equipo. Esto conduce a un problema de control de acceso al medio. Para resumir este problema se da cuando la estación cree que el medio está libre cuando en realidad no lo está, pues está siendo utilizado por otro nodo al que la estación no "oye".

4.1.4 Fragmentation Threshold. En busca de aprovechar y de hacer el mejor uso del ancho de banda prestado por las redes Wireless Lan, se necesitan conocer algunos de los parámetros que permiten la configuración de los protocolos 802.11. Como una opción para nosotros los usuarios, una fuente de transmisión ya sea, una *estación* o *Access point* usa la fragmentación para dividir tramas 802.11 en partes más pequeñas de trama, las cuales son enviadas separadamente a el destinatario. Cada fragmento está compuesto por una capa de cabecera MAC (**MAC Layer Header**), verificador de secuencia de trama (*Frame check Sequence* **FCS**) y un número indicador de la posición del fragmento de trama dentro del global. Debido a que cada fragmento es enviado independientemente por la estación fuente, es el receptor el que se encarga de enviar una réplica de recibido a la fuente (*Acknowledgement*) por cada uno de los fragmentos.

Dentro del campo de control de secuencia de fragmento se encuentra inmerso: la cabecera de cada fragmento y un número de subcampo de fragmento, es decir, es el valor que ocupa el fragmento dentro de la trama. El número es cero para el primer fragmento de la trama, luego este se incrementa en uno por cada fragmento sucesivo de una trama en particular.

La estación de destino reensambla los fragmentos nuevamente en la trama original usando los números encontrados en las cabeceras de cada trama. Luego de asegurarse de que la trama esta completa, la estación envía la trama hacia las capas superiores para su procesamiento.

Para resumir la fragmentación de tramas es básicamente una técnica o parámetro que se configura y que consiste en la división de una trama de un tamaño específico en un número de tramas de valores más pequeños que la trama original, con el fin de evitar el mayor número de colisiones que se puedan presentar en la transmisión de la información que esta contenga. El uso de este parámetro incrementa la confiabilidad de la transmisión de la trama por medio de la variación en el tamaño del paquete a transmitir, el cual puede estar entre los 256 bytes y 2,028 bytes. Se pueden presentar dos casos:

- Si la trama que la fuente (estación, punto de acceso...) esta transmitiendo es mas larga que el estipulado en el parámetro de Fragmentación, entonces este parámetro entrara en funcionamiento.
- Si el tamaño del paquete transmitido es igual o menor que el estipulado en el parámetro de Fragmentación, entonces la fuente no utilizara la función de fragmentación.

4.1.5 RTS / CTS. Request To Send, Clear To Send es un mecanismo usado por la 802.11 protocolo de redes inalámbrico para reducir la colisión de tramas, introducido debido a problemas como: el terminal oculto y el nodo expuesto.

Un nodo que desea enviar datos inicia el proceso enviando una trama de *permiso para enviar* **RTS**. El nodo destino responde con una trama de *listo para recibir* **CTS**. Cualquier otro nodo que reciba la trama de

CTS, se abstiene de enviar datos por un periodo de tiempo (resolviendo así el problema del terminal oculto). La cantidad de tiempo que el nodo debe esperar antes de tener acceso al medio es incluido en las tramas de **RTS / CTS**. Cualquier otro nodo recibiendo la trama **RTS** pero no la trama **CTS** se le permite transmitir a los nodos vecinos (resolviendo el problema del terminal expuesto). Este protocolo fue diseñado asumiendo que todos los nodos tienen el mismo rango de transmisión.

El tamaño de las tramas **RTS / CTS** varía de 0 a 2347 cada una. Si el paquete que el nodo quiere transmitir es mayor que el tamaño del paquete **RTS / CTS**, el mecanismo es activado. Por otro lado, si el tamaño del paquete que el nodo quiere transmitir es igual o menor que el tamaño de la trama **RTS / CTS**, el paquete de datos es enviado inmediatamente.

4.1.6 Ethernet es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, aunque actualmente se llama Ethernet a todas las redes cableadas que usen el formato de trama descrito más abajo, aunque no tenga CSMA/CD como método de acceso al medio.

Esta tecnología fue estandarizada por la especificación IEEE 802.3, que define la forma en que los puestos de la red envían y reciben datos sobre un medio físico compartido que se comporta como un bus lógico, independientemente de su configuración física. Originalmente fue diseñada para enviar datos a 10 Mbps, aunque posteriormente ha sido perfeccionada para trabajar a 100 Mbps, 1 Gbps o 10 Gbps y se habla

de versiones futuras de 40 Gbps y 100 Gbps. En sus versiones de hasta 1 Gbps utiliza el protocolo de acceso al medio CSMA/CD (*Carrier Sense Multiple Access / Collision Detect* - Acceso múltiple con detección de portadora y detección de colisiones). Actualmente Ethernet es el estándar más utilizado en redes locales/LANs.

El diseño original funcionaba a 1 Mbps sobre cable coaxial grueso con conexiones vampiro (que "muerden" el cable) en 10Base5. Para la norma de 10 Mbps se añadieron las conexiones en coaxial fino (10Base2, también de 50 ohmios, pero más flexible), con tramos conectados entre sí mediante conectores BNC; par trenzado categoría 3 (10BaseT) con conectores RJ45, mediante el empleo de hubs y con una configuración física en estrella; e incluso una conexión de fibra óptica (10BaseF).

Los estándares sucesivos (100 Mbps o Fast Ethernet, Gigabit Ethernet, y 10 Gigabit Ethernet) abandonaron los coaxiales dejando únicamente los cables de par trenzado sin apantallar (UTP - *Unshielded Twisted Pair*), de categorías 5 y superiores y la fibra óptica.

Ethernet es la capa física más popular de la tecnología LAN usada actualmente. Otros tipos de LAN incluyen Token Ring 802.5, Fast Ethernet, FDDI, ATM y LocalTalk. Ethernet es popular porque permite un buen equilibrio entre velocidad, costo y facilidad de instalación. Estos puntos fuertes, combinados con la amplia aceptación en el mercado y la habilidad de soportar virtualmente todos los protocolos de red populares, hacen a Ethernet la tecnología ideal para la red de la mayoría de usuarios de la informática actual.

Los elementos en una red Ethernet son los nodos de red y el medio de interconexión. Dichos nodos de red se pueden clasificar en dos grandes grupos: **Equipo Terminal de Datos (DTE)** y **Equipo de Comunicación de Datos (DCE)**. Los **DTE** son los dispositivos que generan o son el

destino de los datos, tales como las computadoras personales, las estaciones de trabajo, los servidores de archivos, los servidores de impresión, todos son parte del grupo de estaciones finales. Mientras que los **DCE** son los dispositivos de red intermediarios que reciben y retransmiten las tramas dentro de la red, y pueden ser ruteadores, conmutadores (switch), concentradores (hub), repetidores, o interfaces de comunicación, como un módem o una tarjeta de interfase por ejemplo.

4.1.7 Internet es una red mundial de computadoras interconectadas con un conjunto de protocolos, el más destacado, el TCP/IP. También se usa este nombre como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada.

Cuando se dice *red de redes* se hace referencia a que es una red formada por la interconexión de otras redes menores.

Al contrario de lo que se piensa comúnmente, Internet no es sinónimo de World Wide Web. Ésta es parte de aquella, siendo la World Wide Web uno de los muchos servicios ofertados en la red Internet. La Web es un sistema de información mucho más reciente (1995) que emplea Internet como medio de transmisión.

Algunos de los servicios disponibles en Internet aparte de la Web son el acceso remoto a otras máquinas (SSH y telnet), transferencia de archivos (FTP), correo electrónico (SMTP), boletines electrónicos (news o grupos de noticias), conversaciones en línea (IRC y chats), mensajería instantánea, transmisión de archivos (P2P, P2M, Descarga Directa), etc.

4.1.8 CSMA/CD. Siglas que corresponden a Carrier Sense Multiple Access with Collision Detection (en español, "Acceso Múltiple con Escucha de Portadora y Detección de Colisiones"), es una técnica usada en redes Ethernet para mejorar sus prestaciones. Primeramente apareció la técnica CSMA, que fue posteriormente mejorada con la aparición de CSMA/CD.

En el método de acceso CSMA/CD, los dispositivos de red que tienen datos para transmitir funcionan en el modo "escuchar antes de transmitir". Esto significa que cuando un nodo desea enviar datos, primero debe determinar si los medios de red están ocupados.

CSMA (Carrier Sense Multiple Access, acceso múltiple con escucha de portadora) significa que se utiliza un medio de acceso múltiple y que la estación que desea emitir previamente escucha el canal antes de emitir. Si el canal está ocupado espera un tiempo aleatorio y vuelve a escuchar. Cuando detecta libre el canal puede actuar de dos formas distintas: emitiendo de inmediato o esperando un tiempo aleatorio antes de emitir. Si emite con una probabilidad p , se dice que es un sistema CSMA p -persistente, mientras que si emite de inmediato se dice que es un sistema CSMA i -inmediato. Una vez comenzado a emitir, no para hasta terminar de emitir la trama completa. Esto supone que se puede producir una colisión si dos estaciones intentan transmitir a la vez, de forma que las tramas emitidas por ambas serán incompresibles para las otras estaciones y la transmisión habrá sido infructuosa.

Finalmente CSMA/CD supone una mejora sobre CSMA, pues la estación está a la escucha a la vez que emite, de forma que si detecta que se produce una colisión para inmediatamente la transmisión.

La ganancia producida es el tiempo que no se continúa utilizando el medio para realizar una transmisión que resultará inútil, y que se podrá utilizar por otra estación para transmitir.

El primer paso a la hora de transmitir será saber si el medio está libre. Para eso escuchamos lo que dicen los demás. Si hay portadora en el medio, es que está ocupado y, por tanto, seguimos escuchando; en caso contrario, el medio está libre y podemos transmitir. A continuación, esperamos un tiempo mínimo necesario para poder diferenciar bien una trama de otra y comenzamos a transmitir. Si durante la transmisión de una trama se detecta una colisión, entonces las estaciones que colisionan abortan el envío de la trama y envían una señal de reinicio. Después de una colisión, las estaciones esperan un tiempo aleatorio (tiempo de backoff) para volver a transmitir una trama.

En redes inalámbricas, resulta a veces complicado llevar a cabo el primer paso (escuchar al medio para determinar si está libre o no). Por este motivo, surgen dos problemas que pueden ser detectados:

1. Problema del nodo oculto: la estación cree que el medio está libre cuando en realidad no lo está, pues está siendo utilizado por otro nodo al que la estación no "oye".
2. Problema del nodo expuesto: la estación cree que el medio está ocupado, cuando en realidad lo está ocupando otro nodo que no interferiría en su transmisión a otro destino.

4.1.9 CSMA/CA. En redes informáticas, Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) es un protocolo de control de redes utilizado para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuenta con un modo práctico para transmitir y recibir simultáneamente). Es un método de acceso de red en el cual cada dispositivo señala su intento para transmitir antes de que lo haga realmente. Esto evita que otros dispositivos envíen la información, así evitando que las colisiones ocurran entre las señales a partir de dos o más dispositivos. De esta forma permite a un emisor transmitir en cualquier momento en que el medio no esté ocupado.

En CSMA/CA, tan pronto como un nodo recibe un paquete que deba ser enviado, comprueba que el canal esta libre (que ningún otro nodo este transmitiendo en ese momento). Si el medio o canal esta libre, entonces el paquete es enviado después de esperar por un corto periodo de tiempo; pero si el canal está ocupado, el nodo esperara por un periodo de backoff.

En redes inalámbricas, no se puede escuchar a la vez que se trasmite: no pueden detectarse colisiones.

Técnica: intentar evitarlas: CSMA with Collision Avoidance: - Si el canal está ocupado se espera a que esté libre - Si está libre, se espera un tiempo, y si sigue libre se transmite

4.1.10 Serial Line Internet Protocol (SLIP). El protocolo serial lineal de Internet (SLIP) es una encapsulacion (incluir datos de un protocolo de una capa mayor en un protocolo de capa menor) obsoleta diseñada para trabajar sobre los puertos seriales (interfaz física que utiliza un método en el cual la información se transfiere un bit a la vez). En los PCs, SLIP ha sido reemplazado por el protocolo PPP (Protocolo punto a punto), el

cual es mucho mejor. Sin embargo SLIP todavía es preferido en algunos equipos como los microcontroladores, ya que encapsula los paquetes IP con una pequeña cabecera en su trama.

SLIP modifica el datagrama estándar de Internet agregando un carácter especial denominado "SLIP END" al final de cada datagrama que distingue un datagrama del otro. SLIP requiere una configuración del puerto para trabajar con 8 bits de datos, sin paridad y con hardware de control de flujo. SLIP no provee de detección de errores, dependiendo de los protocolos de las capas de alto nivel para este trabajo.

4.1.11 Distributed Coordination Function (DCF). Este modo de acceso al medio radio permite la transmisión asíncrona de datos. Las estaciones compiten por los recursos radio para transmitir, mediante un mecanismo denominado CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). El funcionamiento es el siguiente: cuando una estación quiere transmitir, escucha el medio, si está ocupado, espera durante un tiempo prefijado (denominado DIFS, Distributed Inter Frame Space), si durante todo este tiempo el medio está libre, la estación puede transmitir. Al igual que otros protocolos de su especie, para disminuir el número de colisiones cuando se espera por estar el canal ocupado, se utilizan tiempos de espera variables, de distribución exponencial, a este método se le conoce como *exponential backoff*.

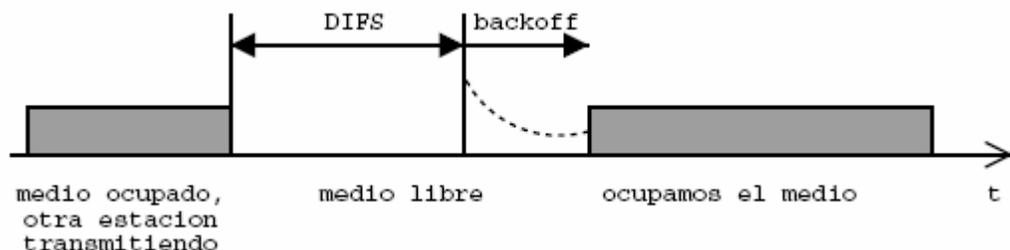


Figura 8. Tiempos de espera para una transmisión, escenario simple.

En la figura 8, se muestra los tiempos de espera que una estación tendrá que respetar a la hora de transmitir. Cada trama enviada es confirmada mediante ACKs. El tiempo de espera que una estación receptora tiene que cumplir para mandar el ACK es mucho mas corto que el DIFS, de forma que se asegura que dos estaciones terminan su dialogo antes de que otra estación intervenga el medio. A este tiempo de espera para mensajes del mismo dialogo se le denomina SIFS (Short IFS). En la figura 9 se muestra un dialogo entre dos estaciones (STA1 y STA2) y una tercera (STA3) que pretende transmitir.

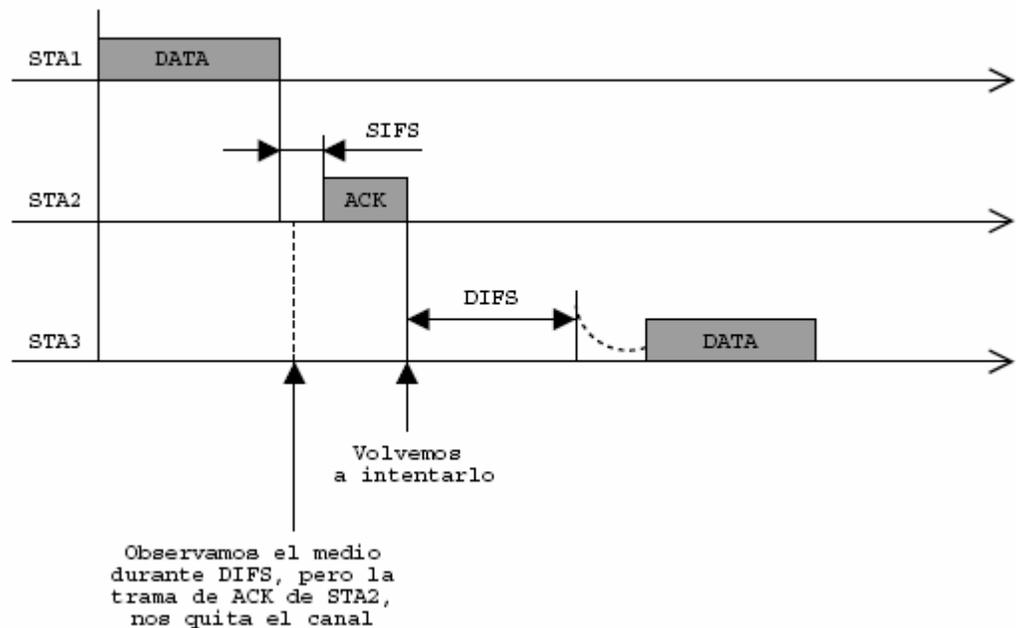


Figura 9. Tiempos de espera para una transmisión, un caso un poco mas complejo

4.1.12 Point Coordination Function (PCF). Este modo de acceso al medio radio permite la transmisión síncrona de datos, lo que dota a las STAs de capacidades de transmisión de datos de tiempo real. En esta configuración, el AP actúa de coordinador del resto de las estaciones, eligiendo quien ha de transmitir en cada momento. El AP tiene prioridad en cuanto al uso del canal, pues no utiliza el DIFS, si no el PIFS (Point

IFS), que es mas corto que el DIFS y mas largo que el SIFS. De esta manera, cuando hay que hacer una asignación de tiempos de transmisión, el AP espera a que se termine la transmisión en curso (que usa SIFS), e interviene el canal (PIFS) mandando la información relevante a las reservas de transmisión. El resto de estaciones han de limitarse a lo que el AP decida. Normalmente tanto el DCF como el PCF conviven a la vez en la red, el AP debe dejar el suficiente tiempo entre los periodos sin contienda, para que las estaciones puedan transmitir datos por acceso distribuido.

4.1.13 SWITCH. Un **switch** (en castellano "conmutador") es un dispositivo electrónico de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconnection*). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones [MAC](#)) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo se dirija únicamente desde el puerto origen al puerto que permite alcanzar el dispositivo destino.

En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

4.1.14 ROUTER. Un **router** (en español *enrutador* o *encaminador*) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo *IP* esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

5 Capitulo 5. PRACTICAS DE WIRELESS SOBRE OPNET

Este capitulo consta de los siete escenarios previamente planteados por medio del simulador de redes OPNET IT GURU ACADEMIA EDITION, en los que se entenderá de manera practica los conceptos base de las redes de comunicación inalámbrica.

5.1 WLAN SIMPLE

1. El primer paso para crear uno de los escenarios a simular será, correr el programa OPNET IT GURU ACADEMIC EDITION.
2. Cuando aparezca la ventana de dialogo > **it Guru Academic Edition** del software, dar clic sobre > **file > New**, en el caso de que el modelo no exista.
3. Al aparecer la ventana de dialogo **New > Project > OK**
4. Aparecerá la ventana de dialogo > **Enter Name**, en la cual se deberá insertar el nombre del proyecto y escenario, Por ejemplo para este caso el *Project Name* será: *wlan_monografia* y el *escenario* será: *wlan simple*.
5. En este momento aparece la ventana de dialogo **Startup Wizard: inicial topology > Create Empty scenario > Next**, luego aparece la ventana de dialogo **Startup Wizard: Cose Network Scale > Office > Next**.
6. **Startup Wizard: Specify Size > Size: meters, X span: 100, Y span: 100 > Next**, luego aparecerán dos ventanas mas de dialogo las cuales se dejaran igual dando click sobre **Next** y **Ok**.
7. Finalmente aparecerá una ventana como la de la figura siguiente (**ventana izquierda**), y colocando click sobre el primer icono de la parte superior izquierda, se mostrara la paleta de objetos (**ventana derecha de la figura**).

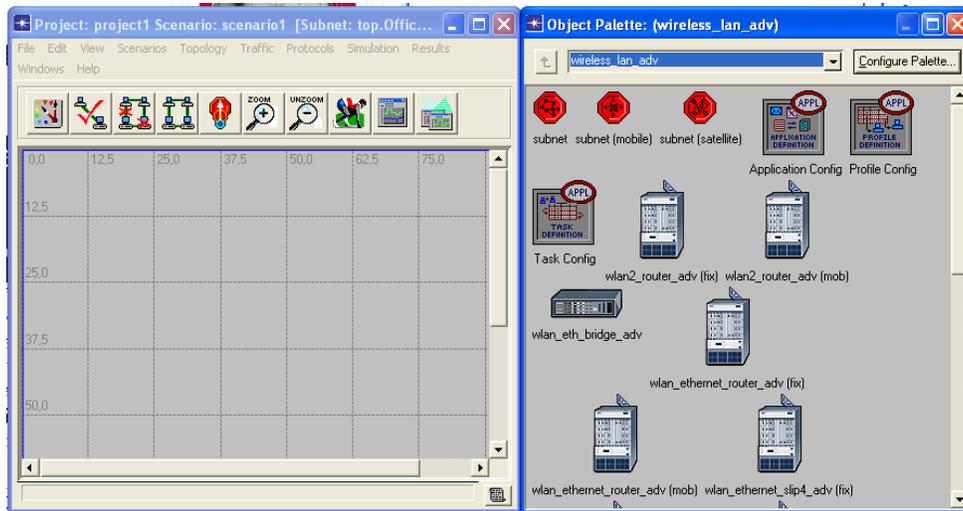


Figura 10. Área de trabajo y Paleta de objetos.

Hasta este momento, se han explicado de manera pausada cada paso necesario para la creación de un modelo en OPNET IT ACADEMIC.

Para este momento deberíamos saber que y cuales son los elementos que se necesitan para poder crear, simular y de esta forma obtener resultados confiables a partir de nuestra simulación. Para el primer caso lo único necesario son dos *wlan_station_adv* (estaciones de trabajo inalámbricas).



Figura 11. Estación inalámbrica.

El modelo de *wlan_station_adv* presentado por OPNET IT, es simplemente una estación de trabajo inalámbrica con el protocolo IEEE 802.11. Este modelo consiste en una fuente de tráfico activo/inactiva. Se escoge esta estación para la simulación ya que esta no posee protocolos TCP, ni el de capas mayores. Al no ser afectada por TCP o capas mayores, la estación *wlan_station_adv* refleja de manera mas precisa el funcionamiento de la capa MAC, que son precisamente los

resultados que se desean obtener en una simulación de *Wlan simple*: verificación de la conexión física.

Debemos ahora seleccionar de la **paleta de objetos**: *wlan_station_adv* y proceder a colocar la estación en la respectiva ventana del escenario. Colocaremos para esta simulación dos estaciones de trabajo.

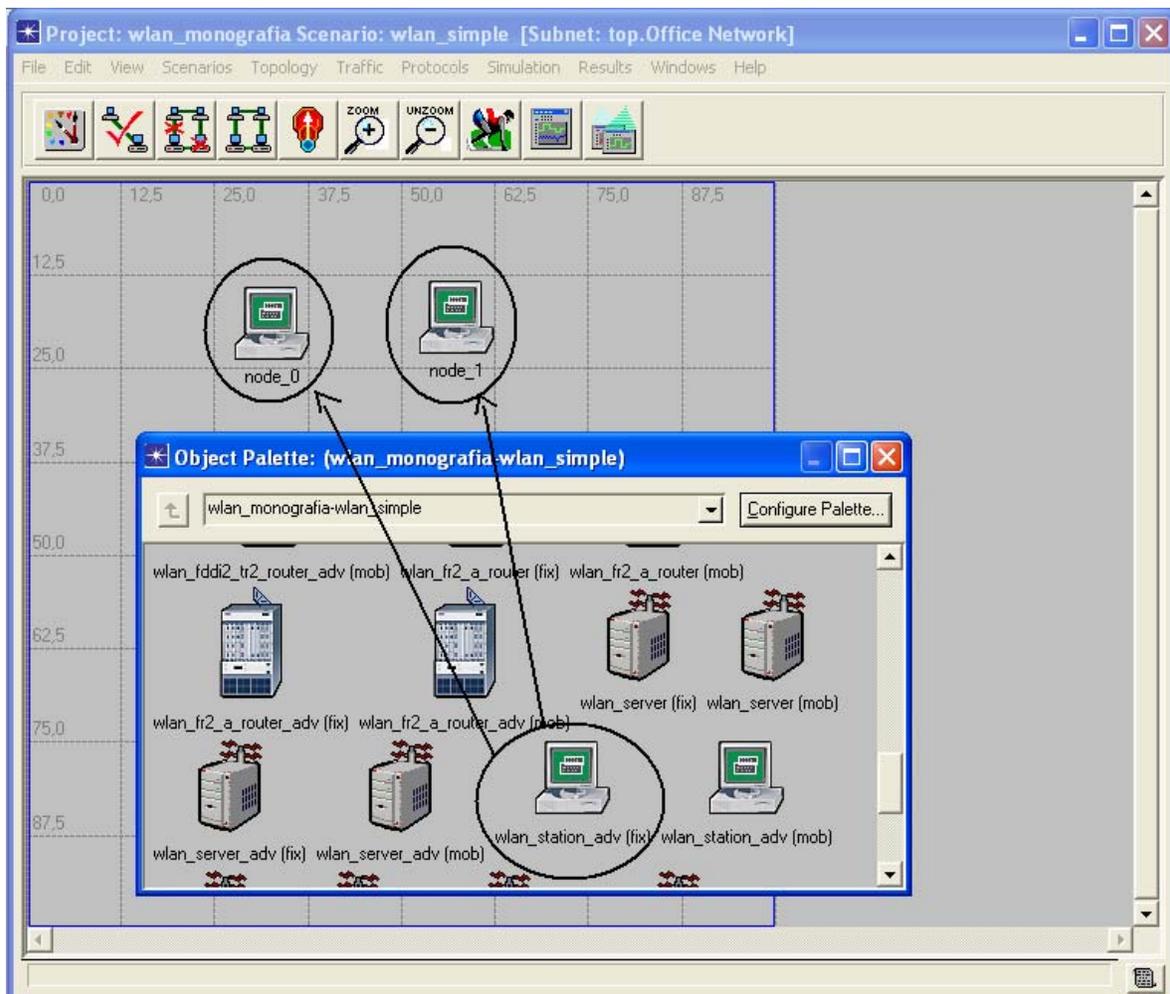


Figura 12. Agregando las estaciones.

Para poder observar una simulación correcta debemos colocar los parámetros de tráfico adecuados:

1. Seleccionar alguna de las estaciones de trabajo Wlan > hacer clic derecho en ella y seleccionar **Select Similar Nodes**.
2. Seleccionar **Edit attributes**.
3. Asignar constant (2) al atributo **Star time**.
4. Asignar never al atributo **Stop time**.
5. Asignar *exponential (0.01)* al atributo **Interarrival time**.
6. Asignar *exponential (150)* al atributo **Packet size**.
7. Asignar *no segmentation* al atributo **Segmentation size**.
8. Asignar *frequency hopping* al atributo **Physical characteristics**.
9. Clic **OK**.

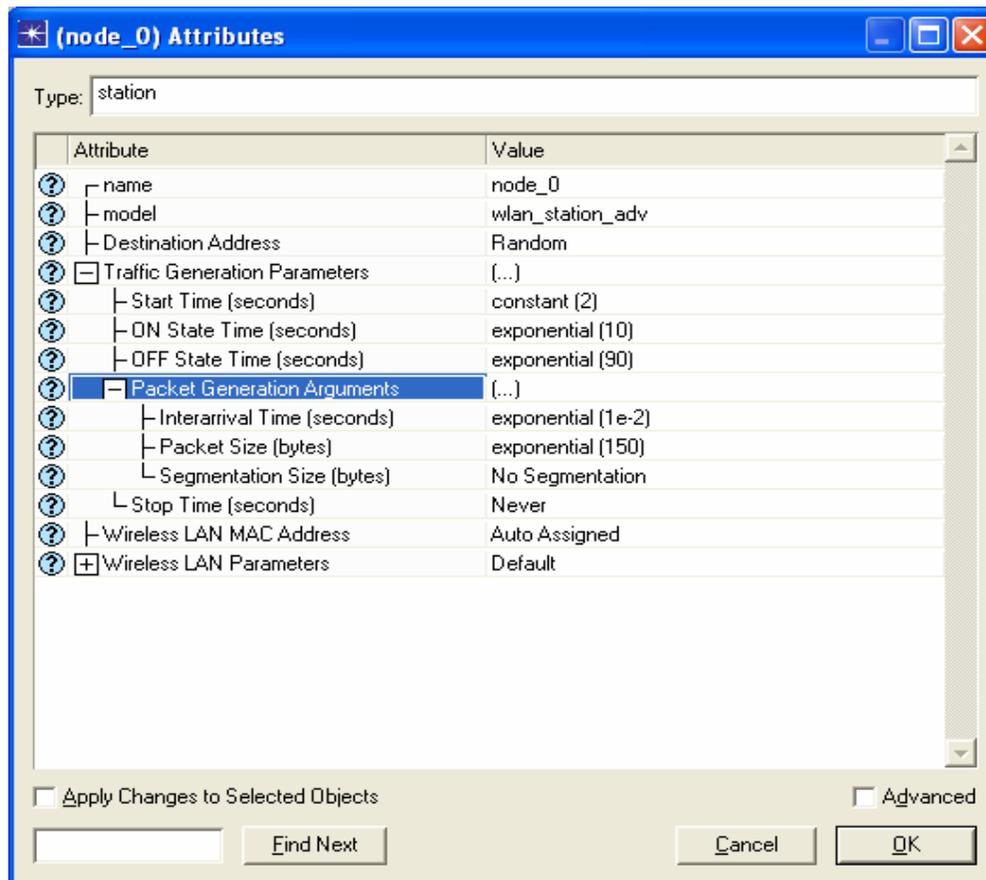


Figura 13. Atributos de una estación.

NOTA: Para realizar la misma configuración para el nodo 1, no se olvide de seleccionar la casilla **Apply Changes to selected Objects** para reflejar los cambios en todos los nodos seleccionados.

Procedemos a obtener los datos deseados, para los cuales debemos:

1. Hacer clic derecho en el área de trabajo de la ventana del editor de proyectos > seleccionar **Choose individual statistics**.
2. Seleccionar **Global statistics > Wireless LAN > todos los parámetros**.
3. Seleccionar **Node statistics > Wireless LAN**.
4. Hacer clic en los parámetros **Media access delay, Load (bits/sec) y Throughput (bits/sec)**.
5. Clic **OK**.

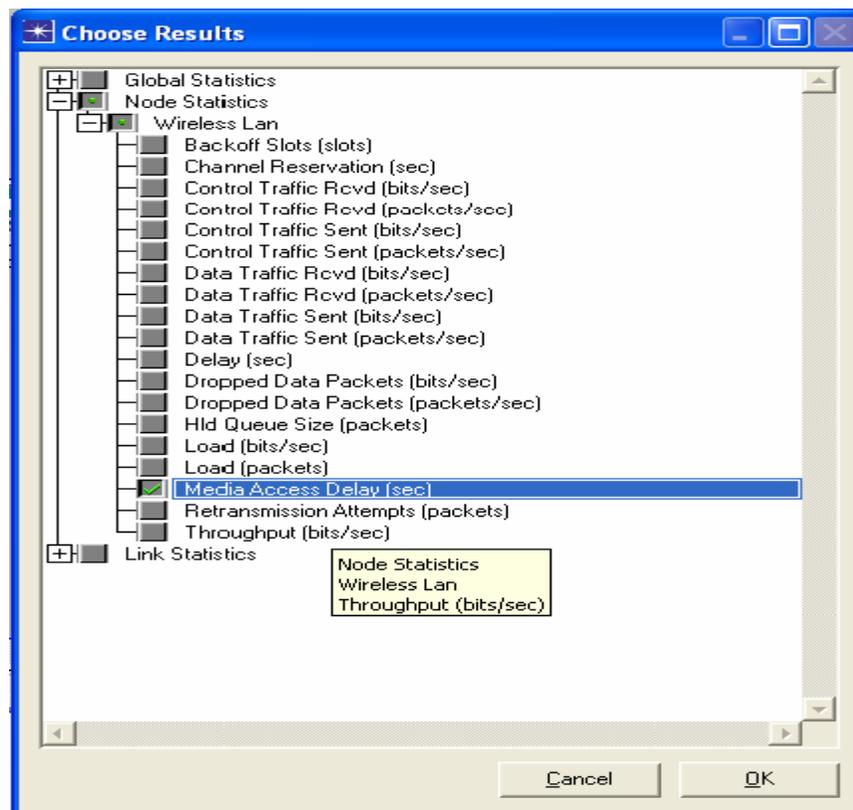


Figura 14. Valores a recolectar de la simulación.

Para configurar y correr los parámetros de la simulación vamos a: configurar / ver simulación.



Figura 15. Configurar simulación en los botones de herramientas.

Simulamos 120 segundos de actividad en la red, para lo cual tecleamos en **Duration** el valor de 120 segundos (valor suficiente para observar las características de una wlan simple). Hacemos clic en **OK** y la simulación se ejecutara.

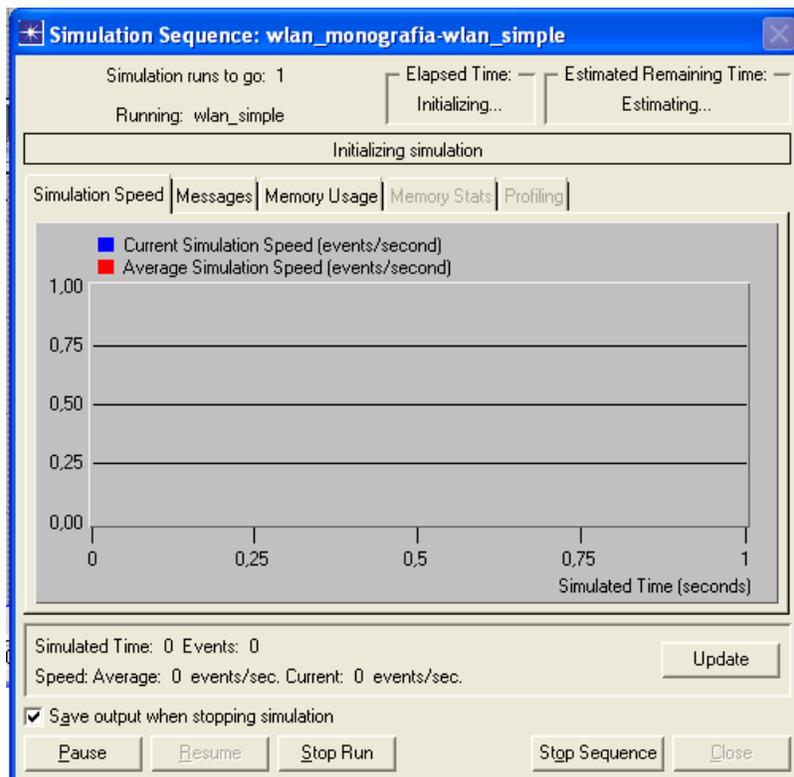


Figura 16. Ventana de proceso de simulación.

Ahora para poder ver los resultados de la simulación, hacemos clic en **view graph and tables of collected statistics**.



Figura 17. "Ver simulación" en los botones de herramientas.

En esta ventana podemos observar cada uno de los parámetros previamente seleccionados.

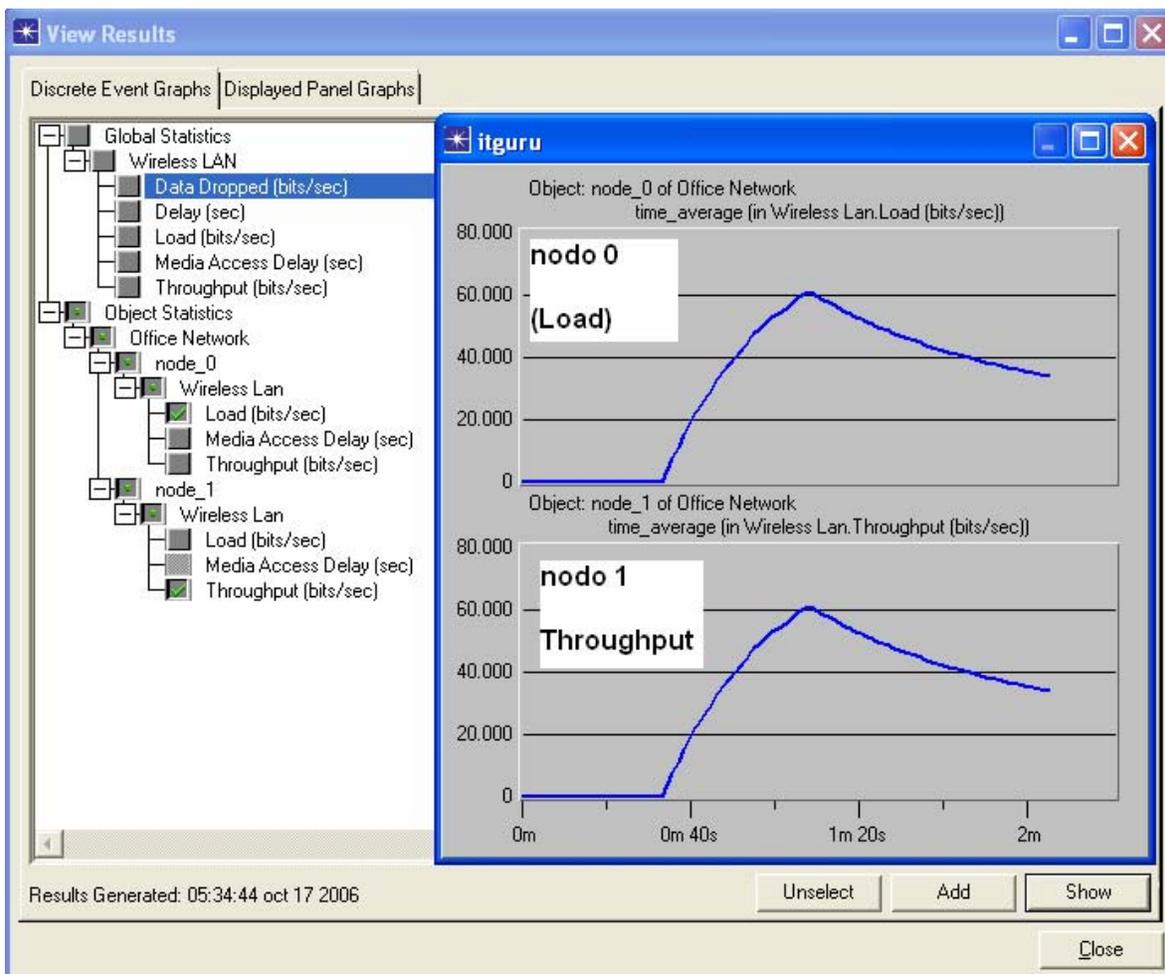


Figura 18. Ventana de selección de resultados y Bits enviados por el nodo_0 vs. Bits recibidos por el nodo_1.

Para observar el comportamiento de la red, obtenemos parámetros como el acceso al medio de los nodos y los datos perdidos durante la utilización de la red.

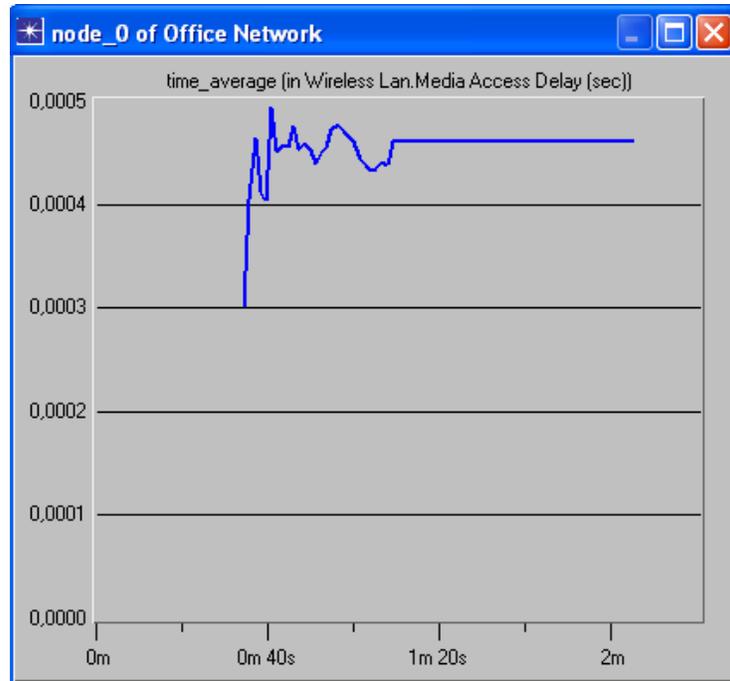


Figura 19. Acceso al medio nodo_0.

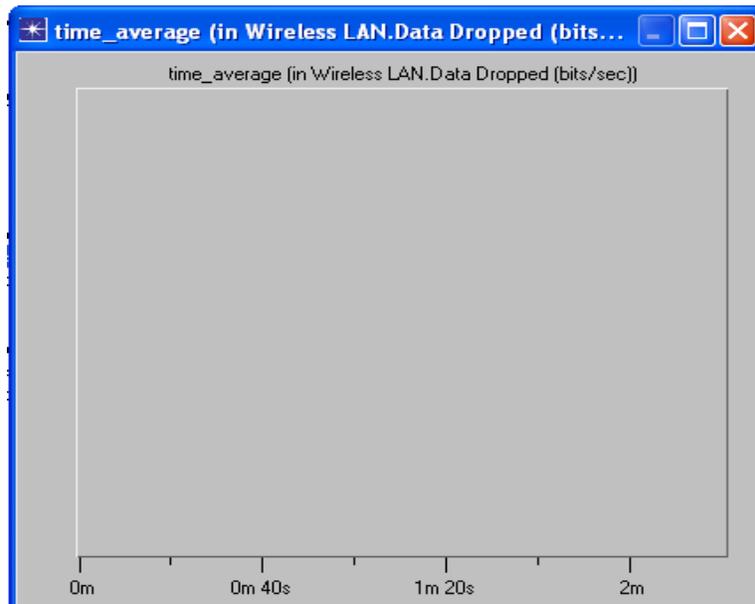


Figura 20. Datos perdidos en la WLAN.

Con el fin de analizar el comportamiento de la red en diversas situaciones observemos ahora el comportamiento de la red con un tamaño del paquete mayor y un tiempo de utilización de la red mucho mayor. Para ello solo modificamos el siguiente parámetro del escenario *wlan_simple*:

Escenario	Parámetros
<i>wlan_simple</i>	<i>Packet Generation arguments</i>
	<i>Packet size = exponential (1024)</i>

Tabla 1. Modificación de las estaciones en *wlan_simple*.

Configuramos un tiempo de simulación de 60 minutos y obtenemos los siguientes resultados: ***Media Access Delay, Load*** y ***Throughput*** de cada uno de los nodos.

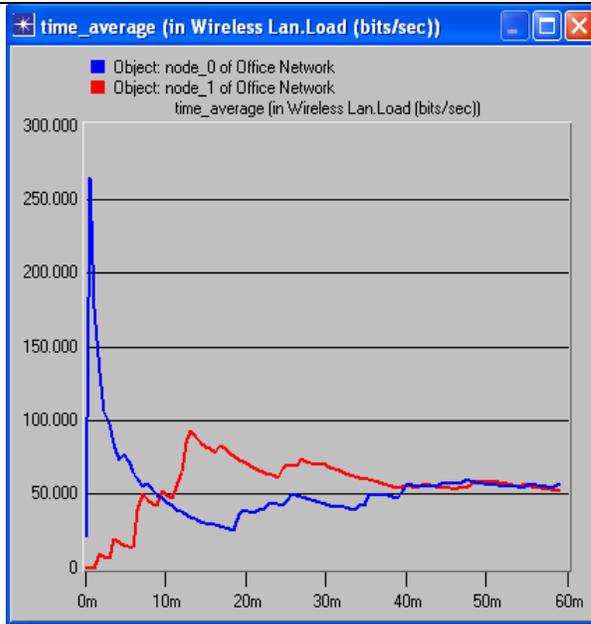


Figura 21. Comparación datos enviados (Load) *nodo0 Vs nodo 1*

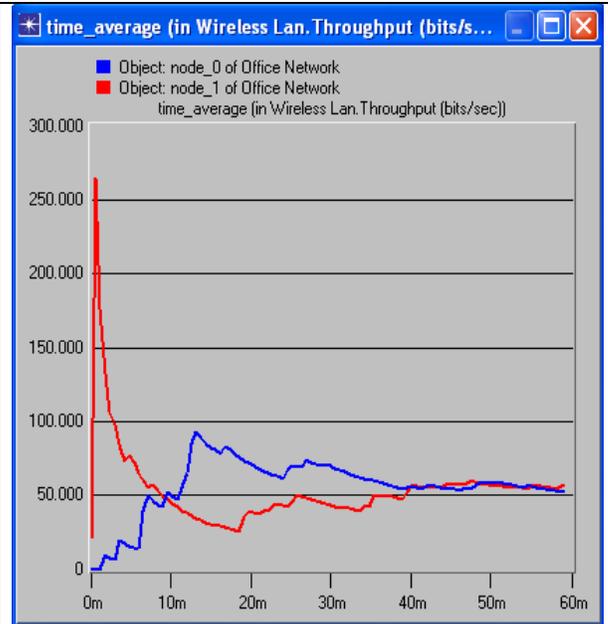


Figura 22. Comparación datos recibidos (Throughput) *nodo0 Vs nodo 1*

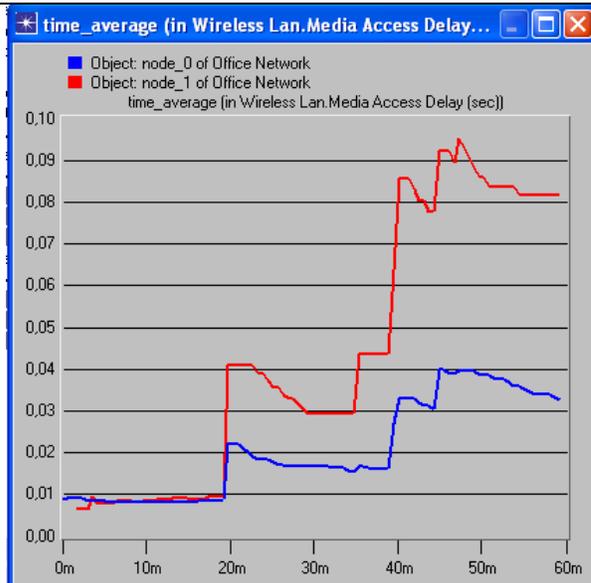


Figura 23. Comparación acceso al medio (Media Access Delay) *nodo0 Vs nodo 1*

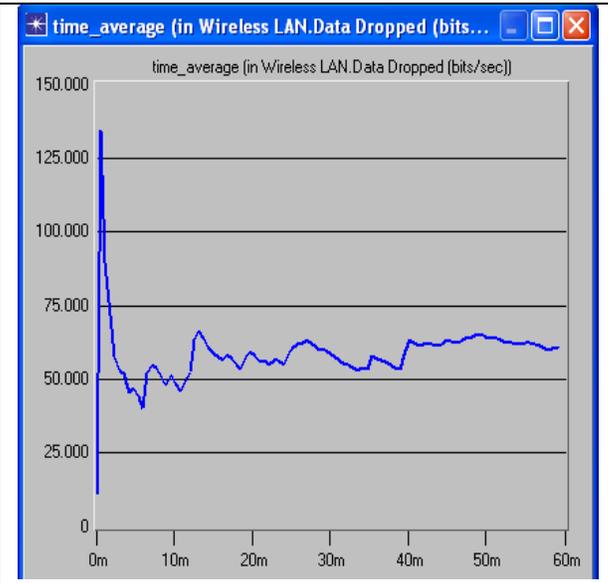


Figura 24. Datos perdidos (Data Dropped) de la red.

Ahora para ver como se comporta un escenario WLAN con varios nodos y bajo diferentes cargas, duplicamos en la opción **Scenario** el escenario *wlan_simple* haciendo clic izquierdo en **Duplicate scenario** y lo nombramos *wlan_simple2*. Duplicamos los nodos, para un total de 5 nodos. Debemos ver algo así:

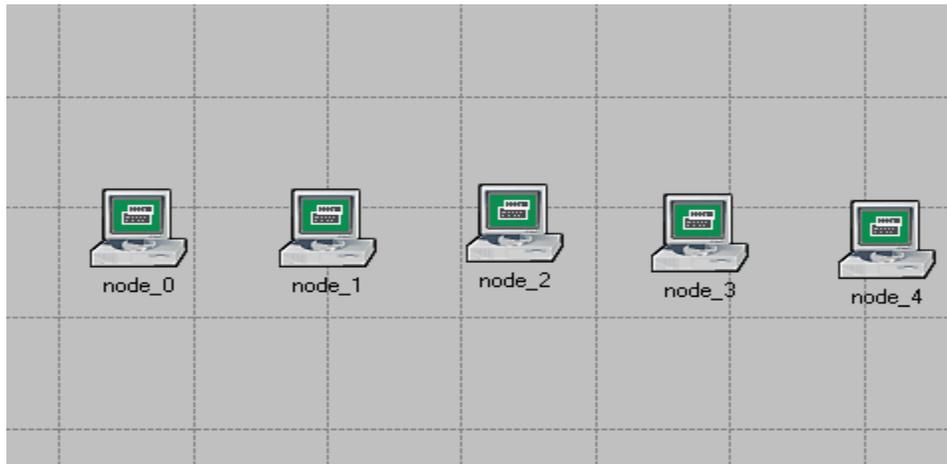


Figura 25. Nuevo escenario: *wlan simple2*.

Para configurar los nodos, hacemos clic derecho en cualquiera de los 5 nodos y seleccionamos **Select similar nodes** para seleccionar todos los nodos. Una vez hecho esto seleccionamos **Edit attributes** para configurar los siguientes parámetros:

Escenario	Parámetros
Wlan_simple2	Traffic Generation Parameters
	<i>Star time (seconds) = constant (2)</i>
	<i>ON State time = exponential (10)</i>
	<i>OFF State time = exponential (90)</i>
	Packet Generation arguments
	<i>Packet size = exponential (1024)</i>
	<i>Interarrival time (seconds) = promoted</i>

Tabla 2. Atributos de las estaciones en *wlan_simple2*.

NOTA: No se olvide de hacer clic en la opción **Apply changes to selected attributes** antes de hacer clic en **OK** para reflejar los cambios en las estaciones, ya que esta opción habilita la configuración realizada para todas las estaciones seleccionadas del escenario.

Para poder promover el parámetro **Interarrival time** a un alto nivel debemos hacer clic derecho en la casilla del valor (**Value**) del parámetro y seleccionar la opción deseada. Recuerde que promover este parámetro nos permite colocar diferentes valores **Interarrival time** y por lo tanto probar el funcionamiento de la red bajo diferentes cargas.

Al finalizar debemos ver una ventana como la siguiente:

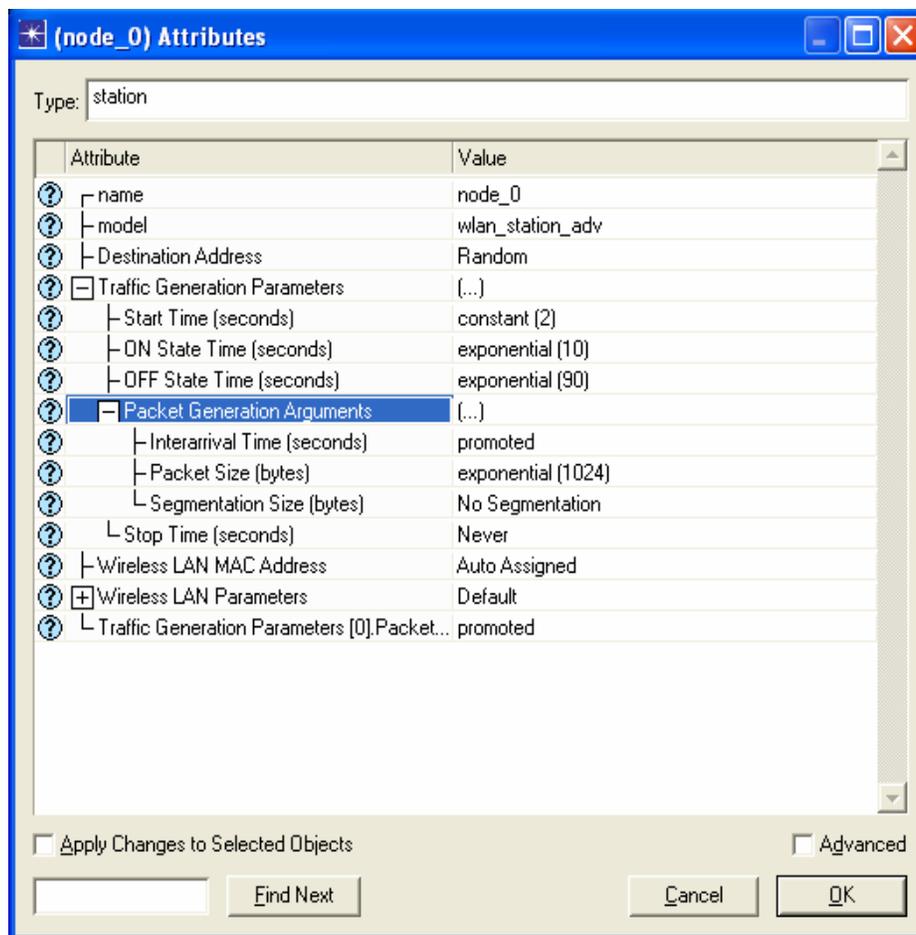


Figura 26. Atributos modificados.

Para examinar el funcionamiento de la red bajo diferentes cargas, usted necesita correr la simulación varias veces cambiando en cada una de las simulaciones la carga de la red. Para poder realizar esto seguimos los siguientes pasos:



1. Hacemos clic derecho en el botón
2. Seleccionamos de la ventana **Common** y asignamos 15 segundos a la duración de la simulación.
3. Hacemos clic en la ventana **Object Attributes**.
4. Hacemos clic en el botón **Add**. La ventana abierta al presionar el botón **Add** debe aparecer llena con los atributos promovidos de todos los nodos de la red. Usted necesita el parámetro **Interarrival time** para todos los nodos. Para hacer eso:
 - a. Hacemos clic en el primer atributo de la lista (**Office Network.Node_0.Traffic ...**) > clic en botón **Wildcard** > clic en **Node_0** de los parámetros que aparecen en la ventana y colocamos * > clic **OK**.
 - b. Un nuevo atributo que contiene el asterisco ha sido generado, adhiéralo haciendo clic en la celda correspondiente de la columna **Add**. Clic **OK**.
 - c. Usted debe ver ahora el atributo generado en la lista de la ventana **Object attributes**.
 - d. Clic en la columna **Value** para colocar los nueve valores que simularan las diferentes cargas de la red.

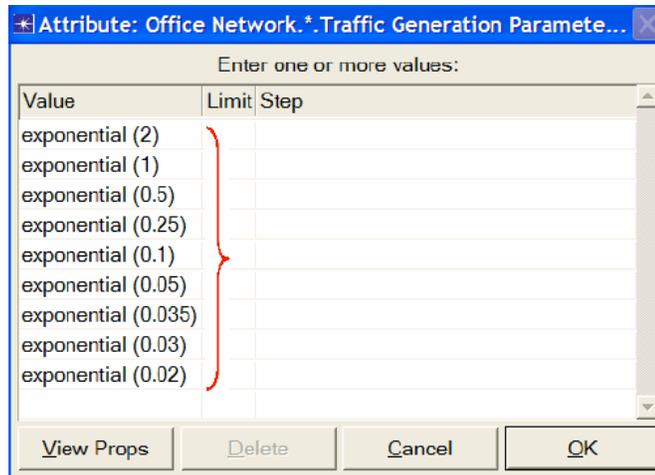


Figura 27. Valores de carga en la red.

e. Una vez terminado debe ver una ventana como la siguiente.

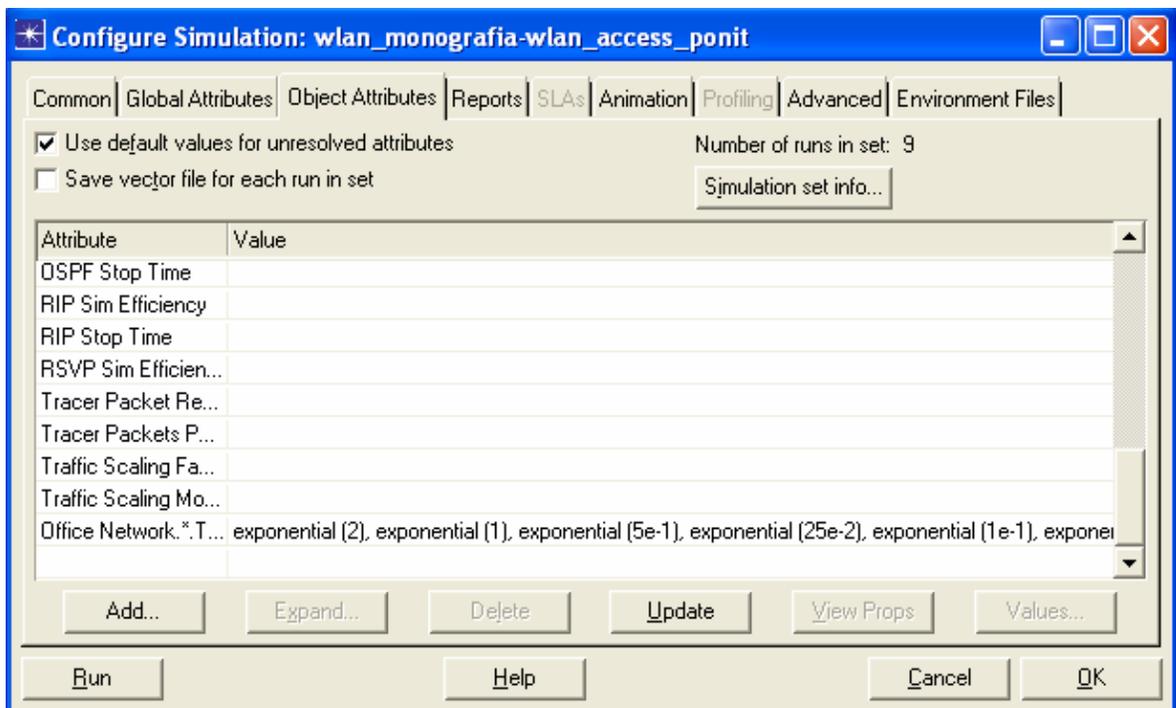


Figura 28. Pantalla de atributos de la simulación.

f. Clic **OK**.

5. Para cada una de las nueve simulaciones, necesitamos salvar un valor escalar que represente el promedio de paquetes enviados en la red (**Load**) y salvar otro valor que represente el promedio de los paquetes recibidos de la red (**Throughput**). Para salvar estos escalares necesitamos configurar el simulador y salvarlos en un archivo. Para hacer esto hacemos clic en la pestaña **Advanced** de la ventana de configuración de simulaciones de OPNET.
6. Debemos ver una ventana como la siguiente, en la que debemos colocar en la opción **Scalar file** el nombre deseado para el archivo.

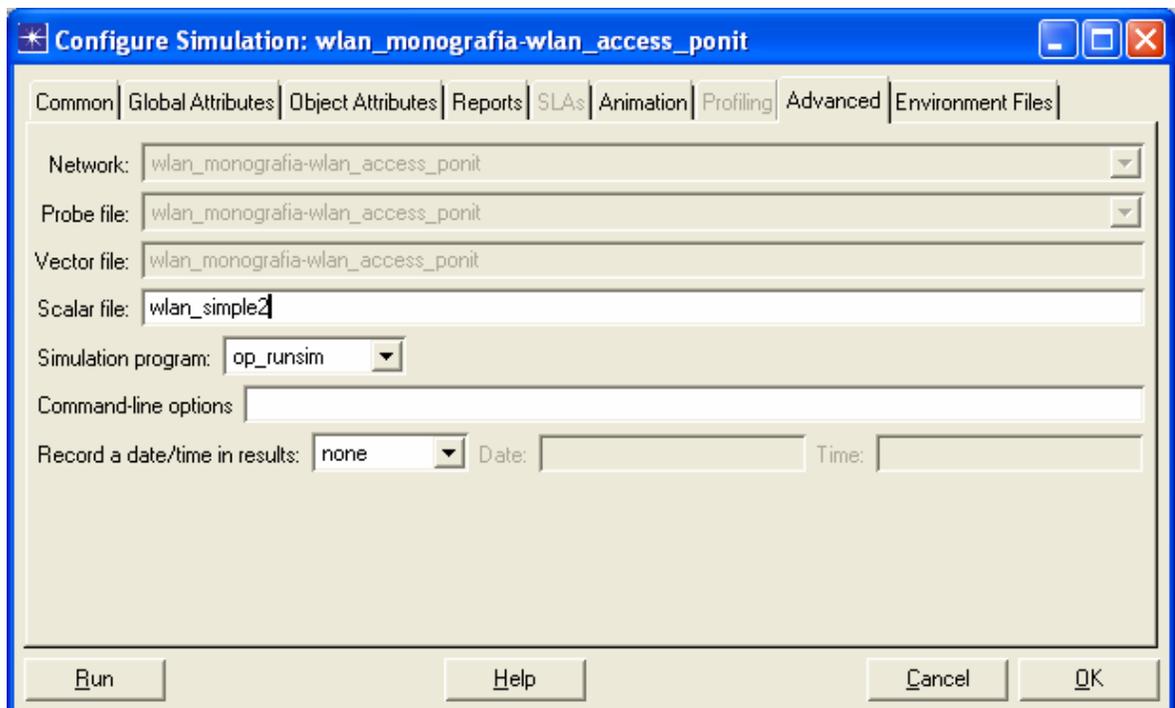


Figura 29. Nombre del vector escalar.

7. Clic **OK** y save el proyecto.

Es de suma importancia recolectar las estadísticas deseadas de la simulación. El primer paso es hacer clic derecho en el área de trabajo del proyecto (sin seleccionar algunos de los nodos o los enlaces) y seleccionar **Choose Individual Statistics** del menú. Colocamos los siguientes parámetros:

Escenario	Parámetros	
Wlan_simple2	Global Statistics	Node Statistics
	Traffic Sink > Traffic Received (packets/sec)	Wireless LAN > Delay (sec)
	Traffic Source > Traffic Sent (packets/sec)	Wireless LAN > Load (bits/sec)
	Wireless LAN > Todos los parámetros	Wireless LAN > Media Access Delay (sec)
	-----	Wireless LAN > Throughput (bits/sec)

Tabla 3. Estadísticas a recolectar del escenario *wlan simple2*.

Ahora para poder recolectar el valor escalar al final de cada simulación:

1. Seleccione **Choose Statistics (Advance)** del menú de simulación.
2. Deben aparecer **Traffic Sent** y **Traffic Received** como opciones de **Global Statistic Probes**.
3. Hacemos clic derecho en **Traffic Received > Edit Attributes**.
4. Habilitamos el valor escalar colocando **enabled** en el parámetro **scalar data**.
5. Habilitamos el tipo de escalar colocando **(time average)** en el parámetro **scalar type**.
6. Comparamos las configuraciones realizadas con la siguiente figura y hacemos clic en **OK**.

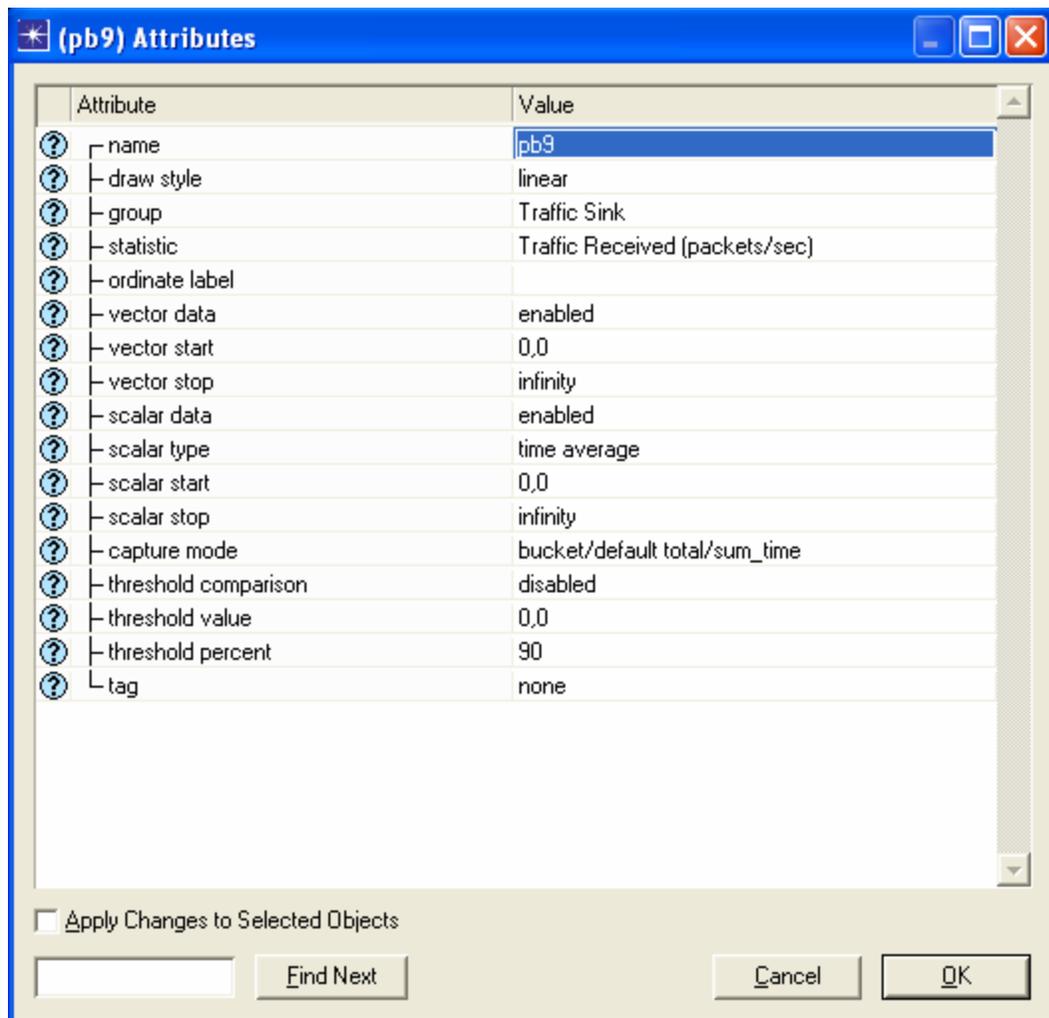


Figura 30. Habilitando el vector escalar.

7. Repetimos los mismos pasos para configurar el parámetro **Traffic Sent** y guardamos el proyecto nuevamente.

Damos un tiempo de simulación de 120 segundos y seleccionamos **View results**



para ver los resultados de las simulaciones. Debemos recolectar diferentes resultados para más adelante obtener conclusiones, el primer resultado a recolectar es el acceso al medio de cada uno de los nodos.

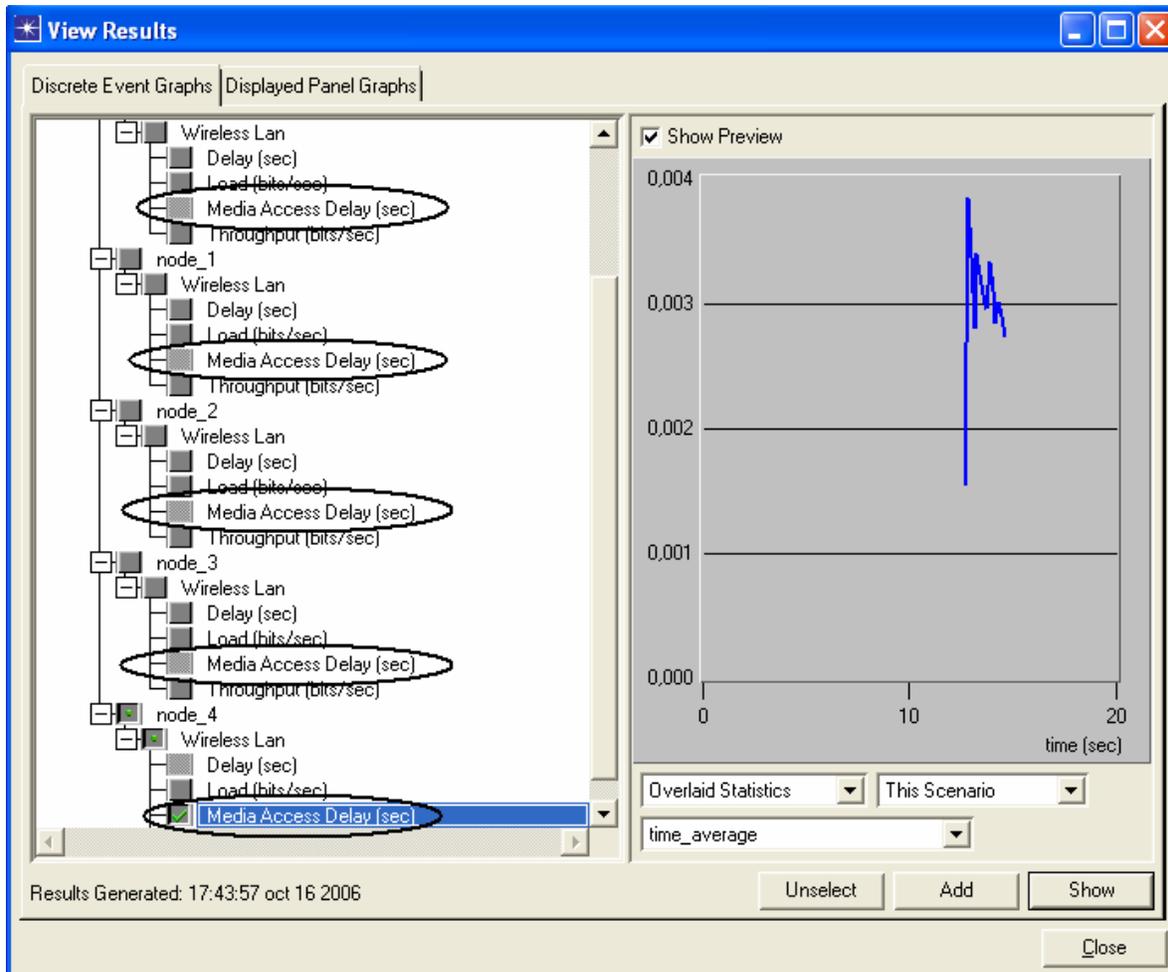


Fig 31. Acceso al medio de cada uno de los nodos.

NOTA: Observemos que el único que tuvo acceso al medio fue el nodo 4.

Recolectemos los resultados de los paquetes enviados (**Load**) de la simulación:

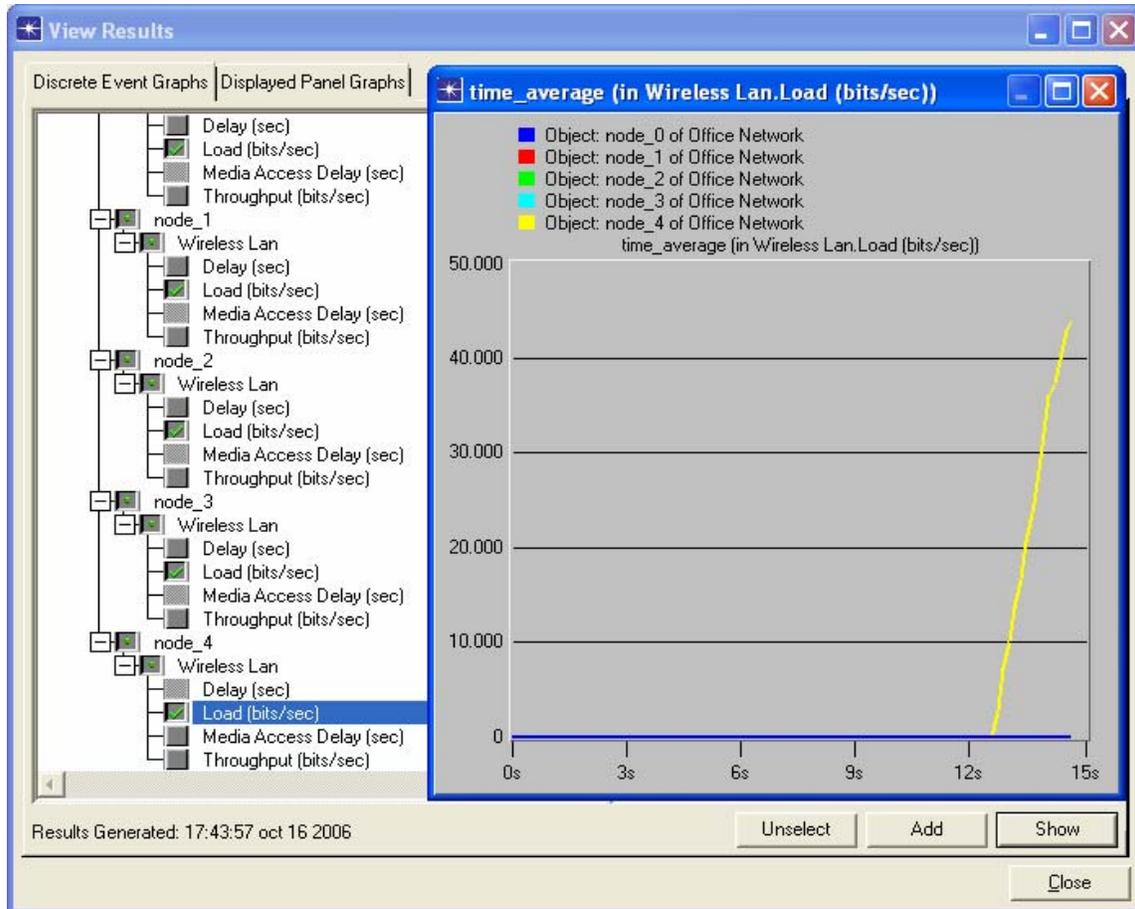


Fig 32. Load de cada uno de los nodos.

NOTA: observamos en la simulación que el único nodo que envió paquetes fue el **nodo 4** (línea amarilla), debido a que fue el único con acceso al medio.

Procedemos ahora con los paquetes recibidos de los nodos:

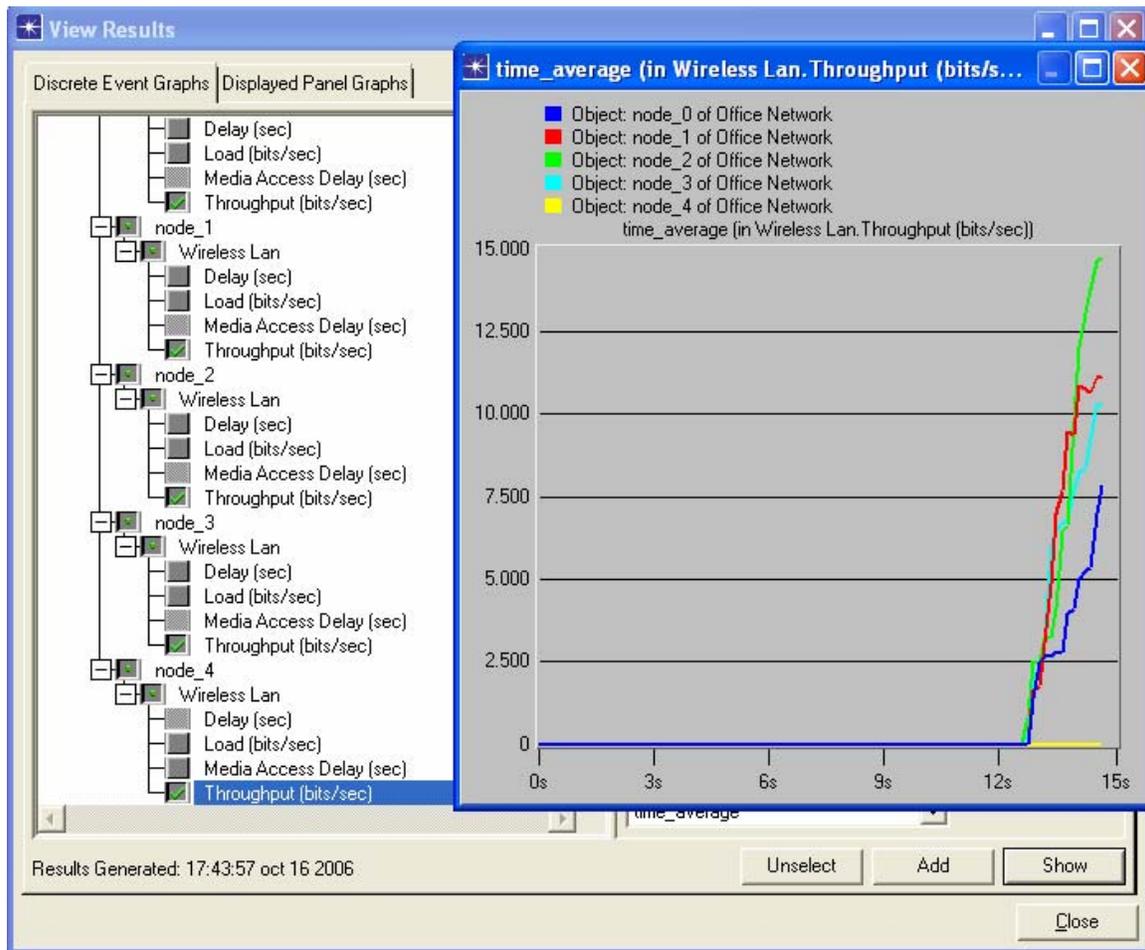


Fig 33. Throughput de cada uno de los nodos.

NOTA: En esta simulación todos los nodos recibieron paquetes excepto el **nodo 4**, ya que como se menciona antes, este nodo fue el encargado de enviar todos los paquetes. Mas adelante analizaremos el porque de esta situación.

Para poder comparar los paquetes enviados y recibidos, debemos seguir los siguientes pasos:

1. Seleccione **View results (Advanced)** del menú **Results**.
2. Ahora que la herramienta **Analisis Configuration** esta abierta. Debemos llamar el valor escalar previamente configurado. Para cargar este valor seleccione **Load Output Scalar File** de la opción **File** del menú y elija el nombre del escalar que eligio, para este caso: **wlan_simple2**.
3. Seleccione **Create Scalar Panel** del menú **Panels**. Asigne **Traffic source. Traffic Sent (packets/sec). Average** a **Horizontal**. Asigne **Traffic sink. Traffic Received (packets/sec)** a **Vertical**. Clic **OK**.

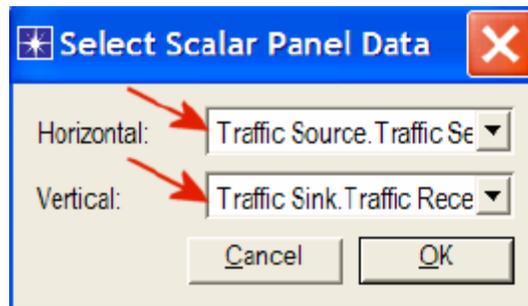


Fig 34. Habilitando el grafico Load Vs Throughput.

4. Debe observar la siguiente grafica:

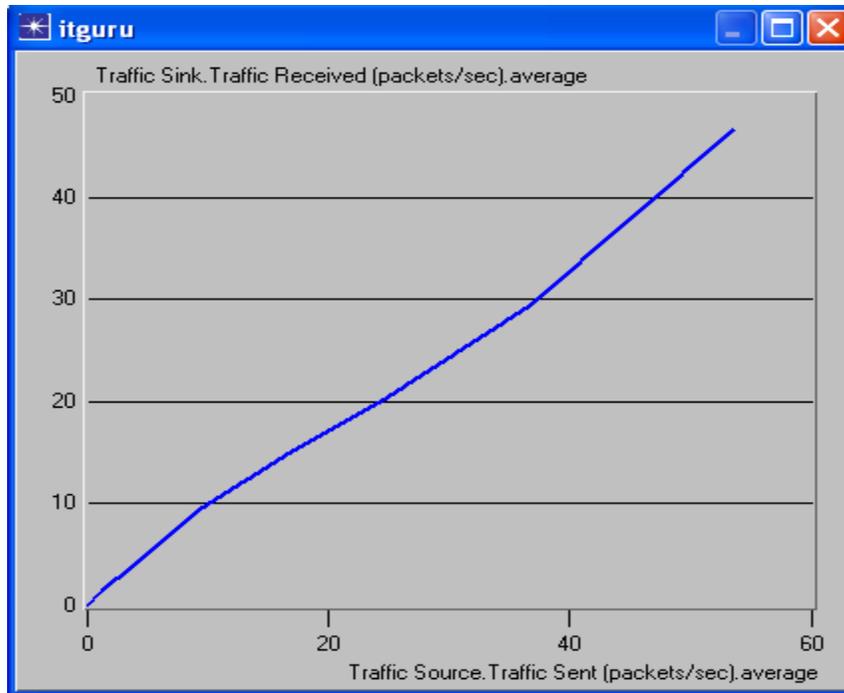


Fig 35. Comparación paquetes enviados (eje X) Vs paquetes recibidos (eje Y) con varias cargas en la red.

El ultimo resultado a recolectar son los datos perdidos **Data Dropped (bits/sec)**. Abrimos el árbol de **Global Statistics** y elegimos el parámetro.

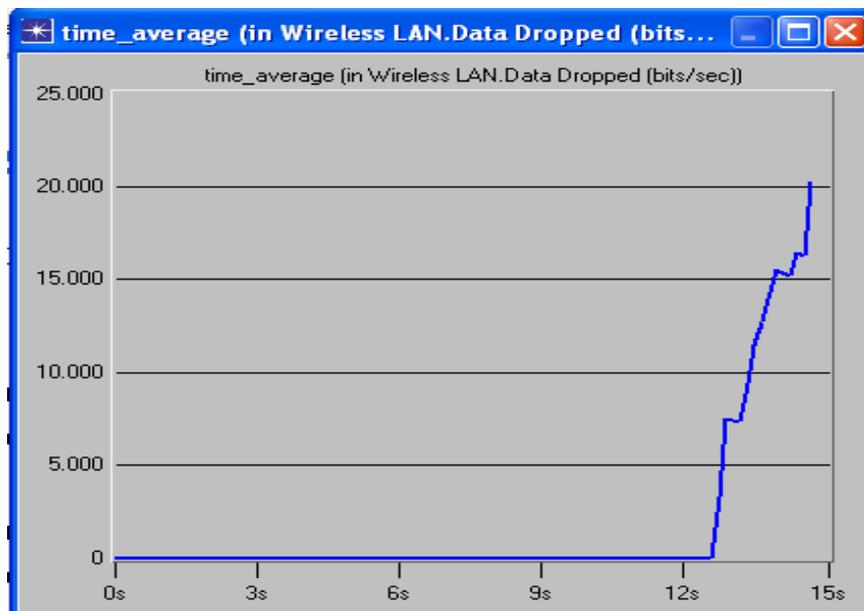


Fig 36. Datos perdidos de la simulación.

5.1.1 Análisis de resultados

Si vemos la figura 18 y 19, podemos observar que el **nodo_0** es el que envía los paquetes en todo momento de la simulación, mientras que el **nodo_1** solo se encarga de recibirlos; esto sucede, ya que el **nodo_0** es el único que tiene acceso al medio (**media access delay**) para enviar los paquetes de datos, y esto ocurre debido a que el tiempo de simulación de 120 segundos solo permitió el tiempo necesario al protocolo **DCF** (que esta activo en todo momento) para que enviara la información del **nodo_0**. Lo que quiere decir que con un poco de más de tiempo de simulación, las dos estaciones (debido al concepto de **DCF**) transmitirán sus datos.

Las estaciones inalámbricas simuladas trabajan bajo la técnica de modulación *frequency hopping* como estaciones de trabajo activo/ inactivo, resultando así un escenario con un tipo de comunicación half-duplex (uno envía y el otro recibe), comprobando nuevamente el funcionamiento del protocolo **DCF**.

Debido a que el tamaño del paquete es pequeño (150bytes), no se pierden datos en la transmisión de los mismos (Figura 20). En este escenario no se presentan problemas como el Terminal oculto o nodo expuesto, debido a que solo hay dos estaciones.

Gracias a la variación realizada en el tamaño del paquete y el tiempo de utilización de la red. En las Figuras 21 y 22, se observa que después de 10 minutos de utilización de la red, la estación inactiva pasa a ser la activa y viceversa, pudiendo de esta forma las dos estaciones acceder al medio en tiempos diferentes (ver Fig 23). También se puede observar que un aumento en el tamaño del paquete disminuye significativamente el desempeño del sistema, ya que los paquetes son demasiado grandes y generan colisiones, por lo que la red decide botarlos (Fig. 24)

Otra conclusión a la cual podemos llegar es que si pudiéramos modificar el **Slot time** (tiempo de espera para que el medio sea libre de transmisiones) de la capa física, es decir, poder modificar los parámetros de la técnica de modulación **Frequency hopping**, observaríamos como a menores valores de **Slot time** se puede mejorar el acceso al medio (**media access delay**), y por lo tanto mejorar el funcionamiento de una red inalámbrica. Lo anterior no se pudo realizar debido a que el software OPNET IT GURU ACADEMIC EDITION no posee las herramientas para modificar la capa física de una simulación.

Para la simulación realizada en donde tenemos una mayor cantidad de nodos (Fig. 25). Observamos otra vez que gracias al tiempo de simulación de 15 segundos, las estaciones trabajan en el modo activo / inactivo por el mecanismo **DCF** y solo el **nodo_4** tiene acceso al medio para enviar los paquetes (ver Fig. 31 y 32). Los demás nodos solo se encargan de recibir la información del **nodo_4** (ver Fig. 33).

Gracias a la simulación de diferentes cargas en la red se puede observar que la figura 35 representa el comportamiento de la red inalámbrica sencilla entre los paquetes enviados y recibidos, vemos que este comportamiento es casi lineal, ya que si observamos detalladamente la gráfica nos podemos dar cuenta de que se envían más paquetes de los que se reciben, por ejemplo para un valor de 40 paquetes enviados, hay un valor aproximadamente de 32 paquetes recibidos, lo que quiere decir que los paquetes enviados son en su mayoría recibidos, lo cual beneficia el funcionamiento de la red. También podemos observar que gracias a que el tamaño del paquete es de 1024 bytes, hay una pérdida de los datos de la red, por lo que podemos concluir que las estaciones WLAN poseen problemas para procesar paquetes de un tamaño considerable, probablemente debido a que el ancho de banda se satura con paquetes tan grandes.

5.2 WLAN SIMPLE CON FRAGMENTACION (FRAGMENTATION THRESHOLD)

En este escenario se pretende mostrar la diferencia entre el enlace simple de dos estaciones inalámbricas y el enlace simple de las mismas estaciones con la fragmentación del paquete enviado.

Para esto creamos un duplicado del escenario *wlan_simple* y lo nombramos *wlan_simple_fragmentacion*. Modificamos la configuración del escenario teniendo en cuenta que el parámetro "**Packet size (bytes)**" tamaño del paquete se encuentre configurado en 1024 bytes en las dos estaciones. Para finalizar habilitamos el parámetro de fragmentación de la siguiente forma:

1. Seleccione alguna de las estaciones de trabajo Wlan > hacer clic derecho > seleccionar > **Select similar nodes** > **Edit attributes**.
2. De los parámetros **Wireless LAN** modifique el parámetro **fragmentation Threshold** a 256 bytes.
3. Modifique el parámetro **Large Packet Procesing** a *Fragment*.
4. **Apply chages to selected objetcs** > Clic **OK**.

En las siguientes figuras se comparan la configuración de una WLAN SIMPLE y una WLAN SIMPLE CON FRAGMENTACION, donde se nota la diferencia de transmisión y recepción de datos cuando se tiene esta característica habilitada en las estaciones inalámbricas.

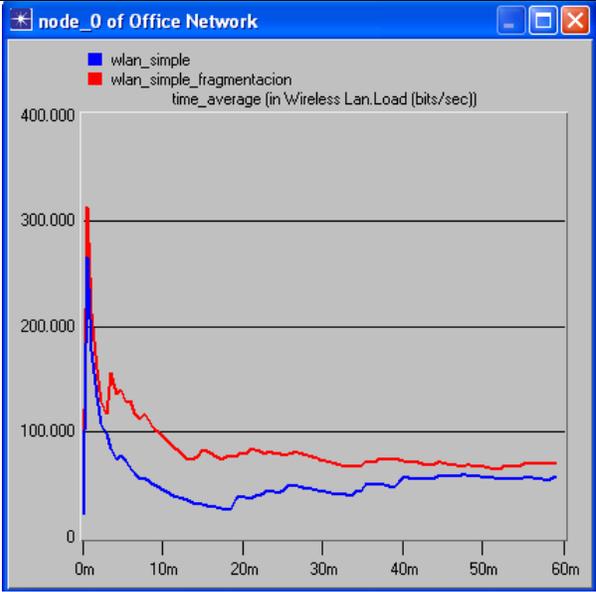


Figura 37. Comparación datos enviados *node0*

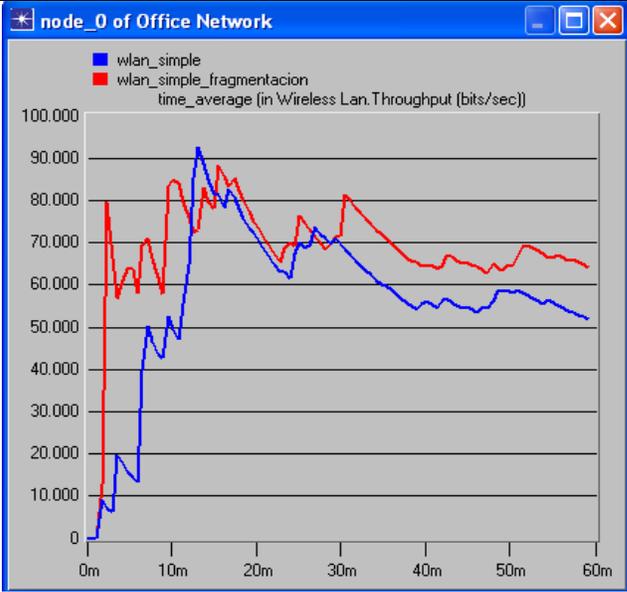


Figura 38. Comparación datos recibidos *node0*

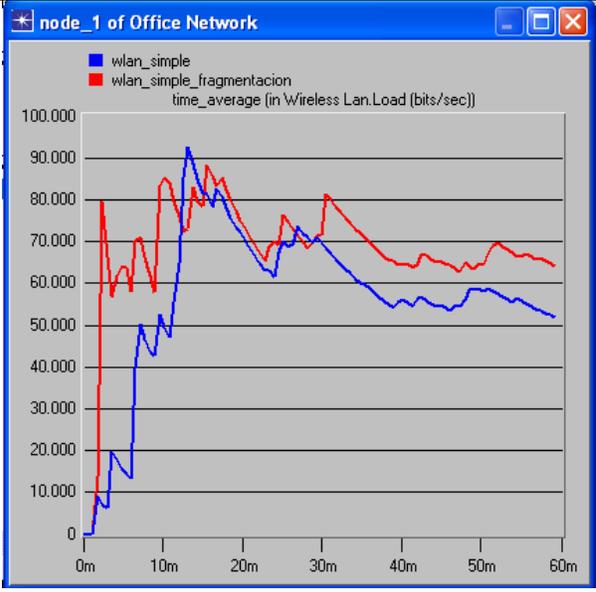


Figura 39. Comparación datos enviados *node1*

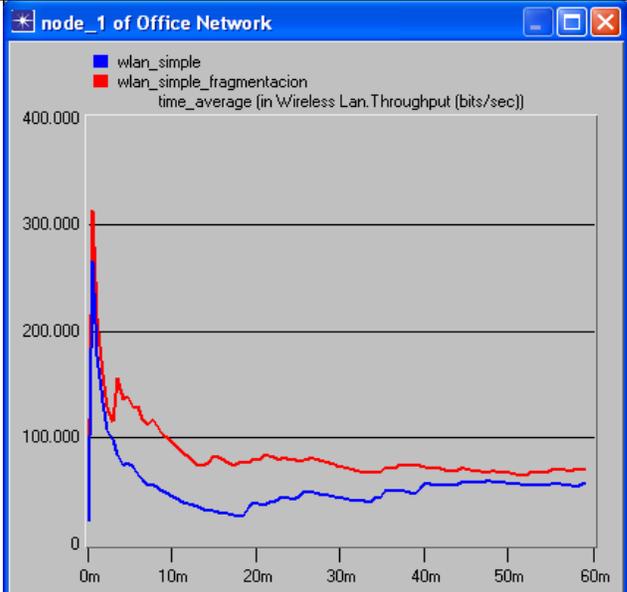


Figura 40. Comparación datos recibidos *node1*

A continuación se compara el acceso al medio de los nodos con y sin fragmentación:

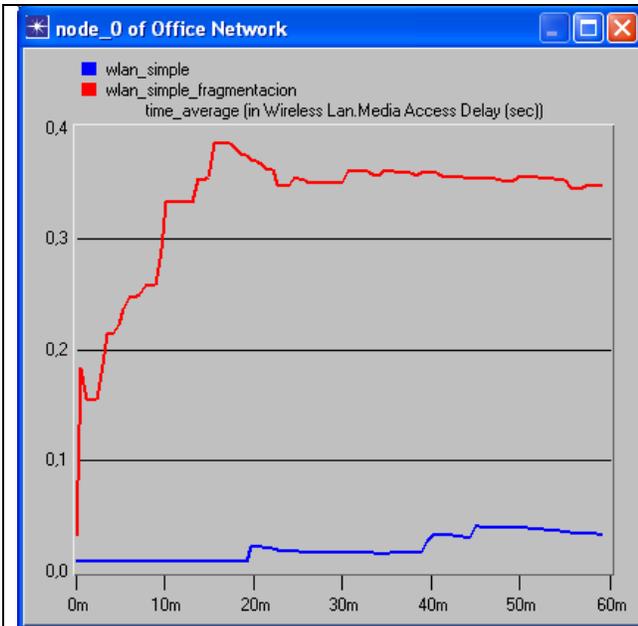


Figura 41. Comparación Acceso al medio
Nodo 0

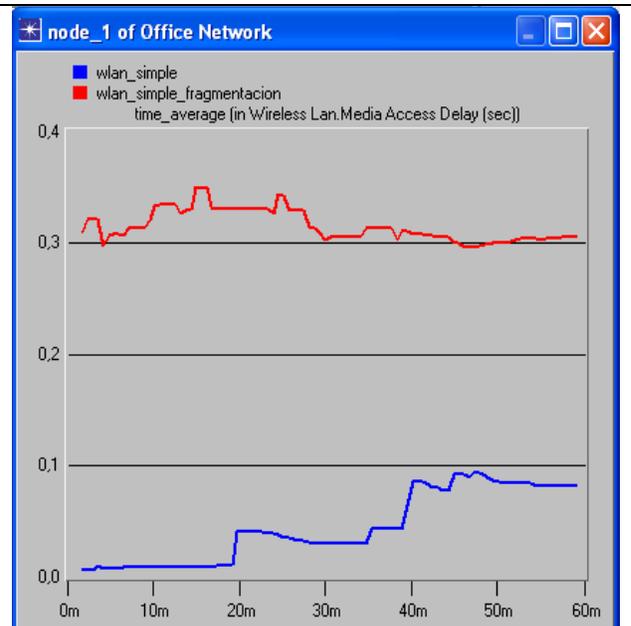


Figura 42. Comparación Acceso al medio
Nodo1

Obtenemos los resultados de la perdida de datos en los escenarios:

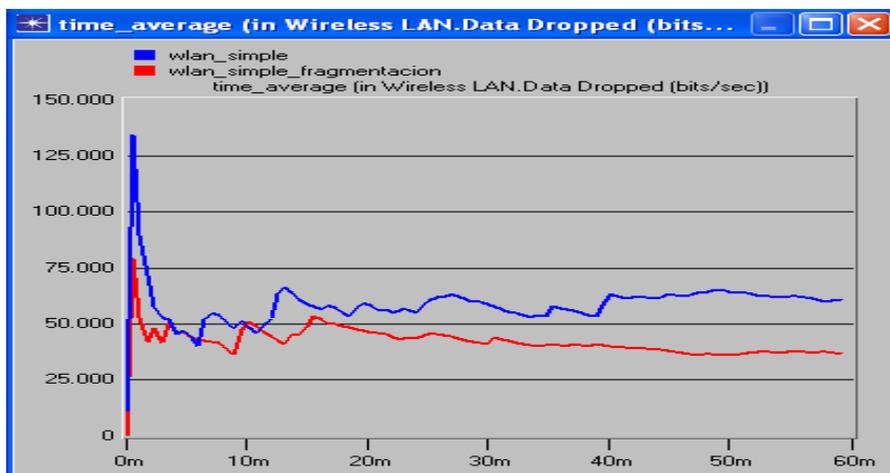


Figura 43. Comparación perdida de datos *wlan_simple* Vs *wlan_simple-fragmentacion*.

5.2.1 Análisis de resultados.

Para los paquetes enviados y recibidos, observando las graficas de las figuras 37,38, 39 y 40 es evidente que activar la fragmentación de tramas aumenta la cantidad de paquetes enviados y recibidos, por lo que podemos concluir que habilitar la fragmentación aumenta el desempeño de la red, aumentando **Load y Throughput**. Pero ojo, no todo es tan perfecto como parece, ya que al observar las graficas de acceso al medio (Figuras 41 y 42) vemos que el retraso de cada nodo para acceder al medio es mayor cuando tiene la fragmentación habilitada. Por lo que para ver si es viable habilitar este mecanismo debemos observar las colisiones de la red.

Observando la figura 43, vemos que las colisiones van disminuyendo para la fragmentación habilitada, mientras que para el otro caso van aumentando. Por lo que podemos concluir que la implementación de este parámetro pueda que involucre un elevado numero de cabeceras en la transmisión de una trama, dando así un mayor retraso para acceder al medio, pero su uso puede resultar en un mejor comportamiento y rendimiento de la red si su configuración se realiza adecuadamente y con un monitoreo constante del flujo de datos.

5.3 WLAN RTS / CTS (Request to send / Clear to send)

En este escenario pretendemos observar el comportamiento de una WLAN ante la activación del mecanismo **RTS / CTS**. Existen dos formas de activar RTS / CTS, numero uno, en las estaciones de trabajo y numero dos, en el punto de acceso.

El primer paso es crear un escenario haciendo clic en **Scenarios**, presionando **New Scenario** y nombrarlo *wlan_rts_cts0*.

Debido a que vamos a probar un mecanismo de control de flujo (RTS / CTS), podemos utilizar las mismas estaciones *Wlan* que se utilizaron en los dos primeros escenarios. Para comprobar como funciona el mecanismo RTS /CTS por medio de OPNET escogemos los siguientes equipos: 5 estaciones *wlan_station_adv*, un servidor ethernet cualquiera y un punto de acceso *wlan_eht_bridge_adv*. Seleccionamos los ítems anteriores de la **paleta de objetos** y los colocamos en el área de trabajo:

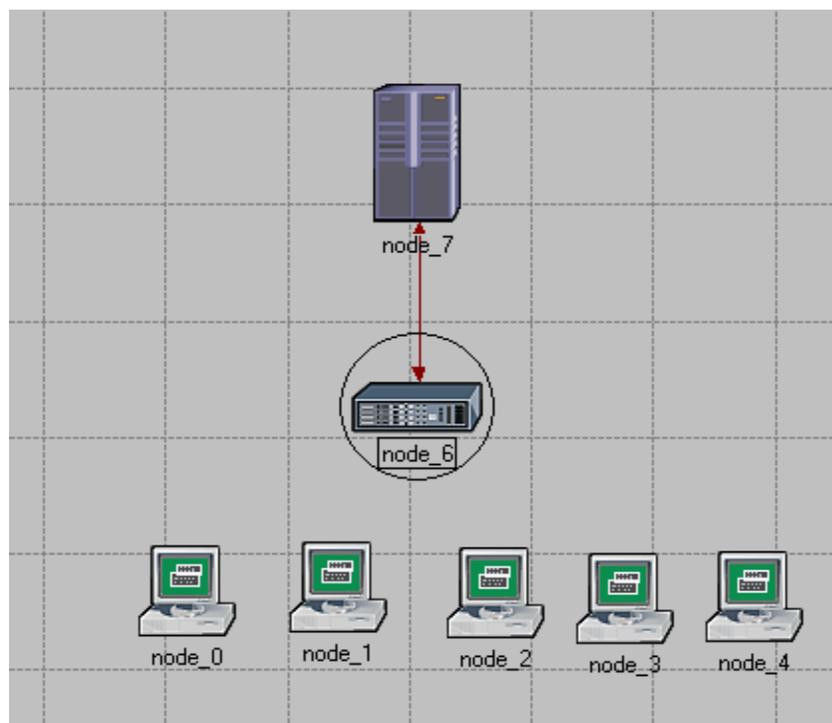


Figura 44. Selección de los equipos para el escenario RTS / CTS.

Primero observaremos como se comporta la red cuando tiene el mecanismo activado en el punto de acceso, por lo que para ello necesitaremos de tres escenarios con diferentes valores del mecanismo. Procedemos entonces a modificar los atributos de los equipos:

Escenario	Parámetros	
<i>Wlan_rts_cts0</i>	Punto de acceso	Estaciones
	<i>Wireless LAN Parameters</i>	
	RTS Threshold = 2000	RTS Threshold = None
	Access point functionality = Enabled	Access point functionality = Disabled
<i>Wlan_rts_cts1</i>	<i>Wireless LAN Parameters</i>	
	RTS Threshold = 256	RTS Threshold = None
	Access point functionality = Enabled	Access point functionality = Disabled
<i>Wlan_rts_cts2</i>	<i>Wireless LAN Parameters</i>	
	RTS Threshold = None	RTS Threshold = None
	Access point functionality = Enabled	Access point functionality = Disabled

Tabla 4. Asignación de los atributos en las redes RTS / CTS en el punto de acceso.

NOTA: Para cada uno de los escenarios colocamos los mismos atributos ***Traffic Generation Parameters y Packet Generation arguments*** vistos en el escenario *wlan_simple*, solo modificamos los parámetros ***Wireless*** mencionados.

Recordemos que antes de correr la simulación debemos colocar las estadísticas o los parámetros de la red que deseamos observar, para lo cual hacemos clic derecho en el área de trabajo y seleccionamos **Choose individual statistics**, colocamos:

Escenario	Parámetros
<i>Wlan_rts_cts0</i>	<i>Global Statistics</i>
	<i>Wireless LAN = Todas</i>
	<i>Node Statistics</i>
	<i>Wireless LAN = Todas</i>
<i>Wlan_rts_cts1</i>	<i>Global Statistics</i>
	<i>Wireless LAN = Todas</i>
	<i>Node Statistics</i>
	<i>Wireless LAN = Todas</i>
<i>Wlan_rts_cts2</i>	<i>Global Statistics</i>
	<i>Wireless LAN = Todas</i>
	<i>Node Statistics</i>
	<i>Wireless LAN = Todas</i>

Tabla 5. Estadísticas a recolectar *wlan_rts_cts1*.

Corremos las simulaciones de los escenarios por un tiempo de simulación de 12 horas (para darle más tiempo de trabajo a la red y más utilización al medio) y obtenemos los siguientes resultados:

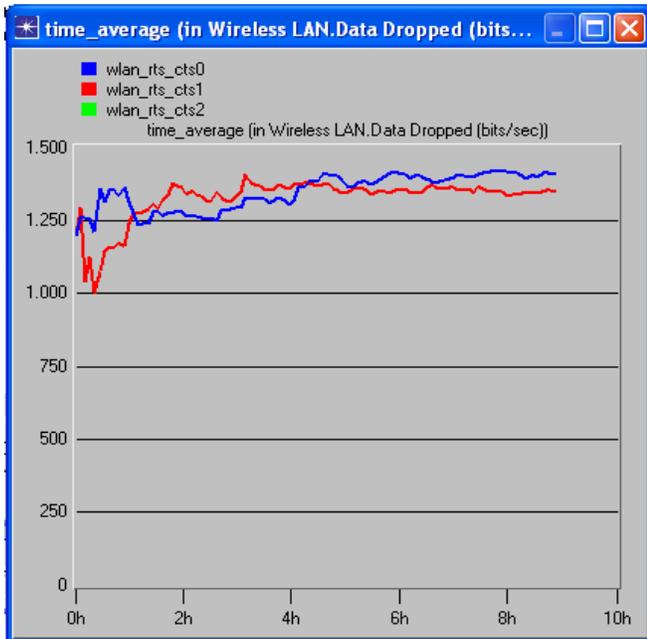


Fig 45. Comparación datos perdidos.

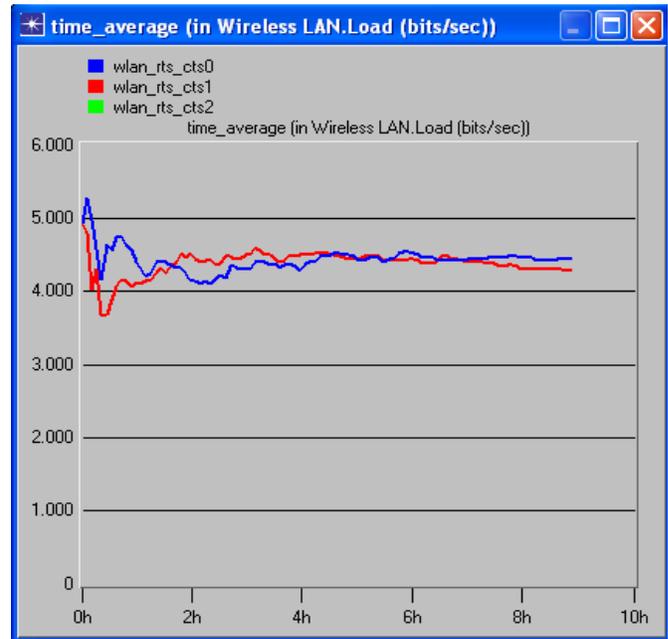


Fig 46. Comparación datos enviados.

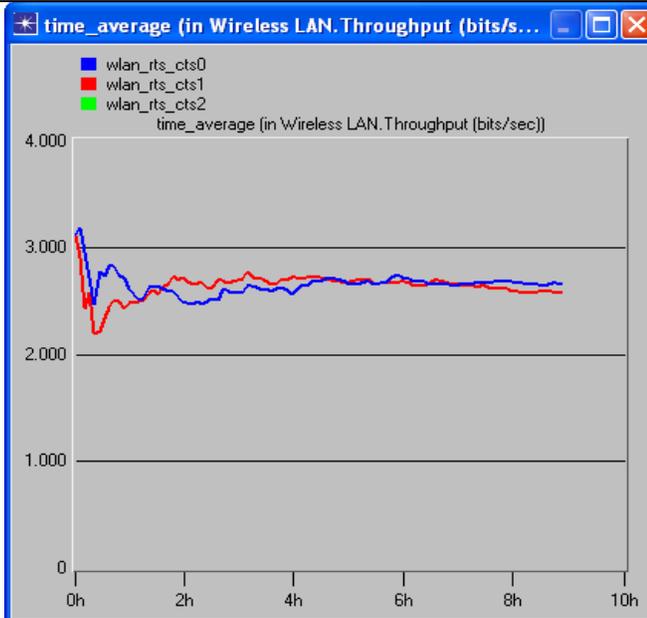


Fig 47. Comparación datos recibidos.

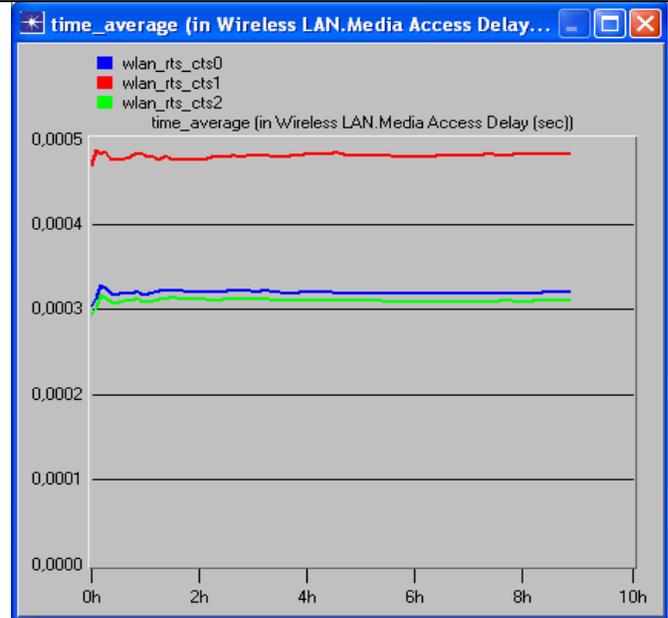


Fig 48. Comparación acceso al medio.

Para obtener más conclusiones acerca de este mecanismo procedemos a simular cuando las estaciones tienen activado el mecanismo y el punto de acceso no. Configuramos los siguientes parámetros:

Escenario	Parámetros	
<i>Wlan_rts_cts3</i>	Punto de acceso	Estaciones
	<i>Wireless LAN Parameters</i>	
	RTS Threshold = None	RTS Threshold = 2000
	Access point functionality = Enabled	Access point functionality = Disabled
<i>Wlan_rts_cts4</i>	<i>Wireless LAN Parameters</i>	
	RTS Threshold = None	RTS Threshold = 256
	Access point functionality = Enabled	Access point functionality = Disabled
<i>Wlan_rts_cts5</i>	<i>Wireless LAN Parameters</i>	
	RTS Threshold = None	RTS Threshold =None
	Access point functionality = Enabled	Access point functionality = Disabled

Tabla 6. Configuración de los atributos en *wlan_rts_cts 3 y 4*.

Recolectamos las siguientes estadísticas:

Escenario	Parámetros
<i>Wlan_rts_cts3</i>	<i>Global Statistics</i>
	<i>Wireless LAN = Todas</i>
<i>Wlan_rts_cts4</i>	<i>Global Statistics</i>
	<i>Wireless LAN = Todas</i>
<i>Wlan_rts_cts5</i>	<i>Global Statistics</i>
	<i>Wireless LAN = Todas</i>

Tabla 7. Configuración de las estadísticas en *wlan_rts_cts 3 y 4*.

Corremos las simulaciones y obtenemos los siguientes resultados:

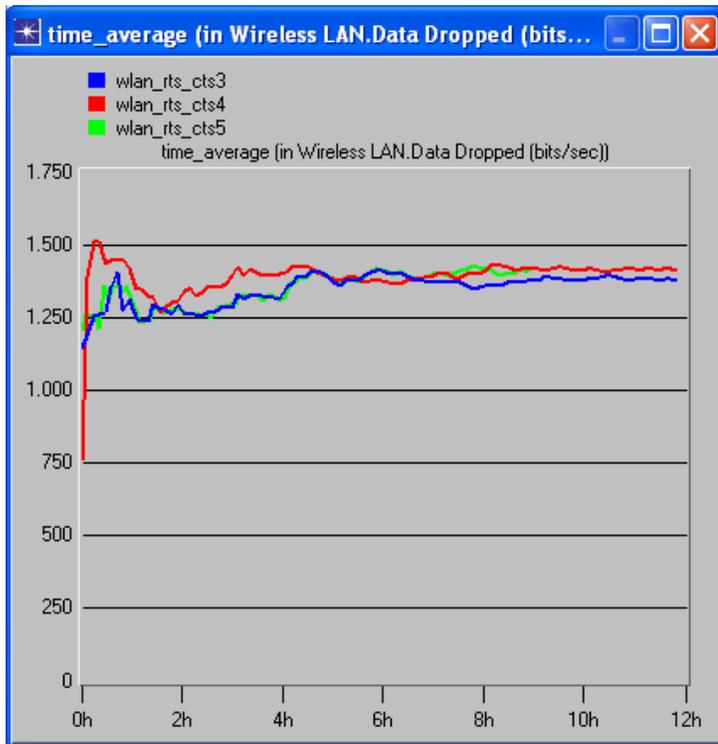


Fig 49. Comparación de datos perdidos.

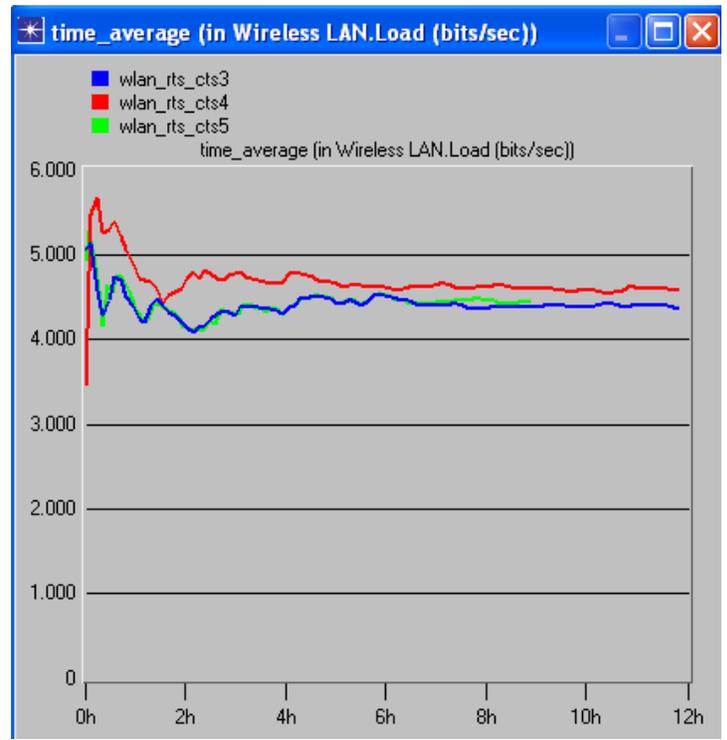


Fig 50. Comparación de datos enviados.

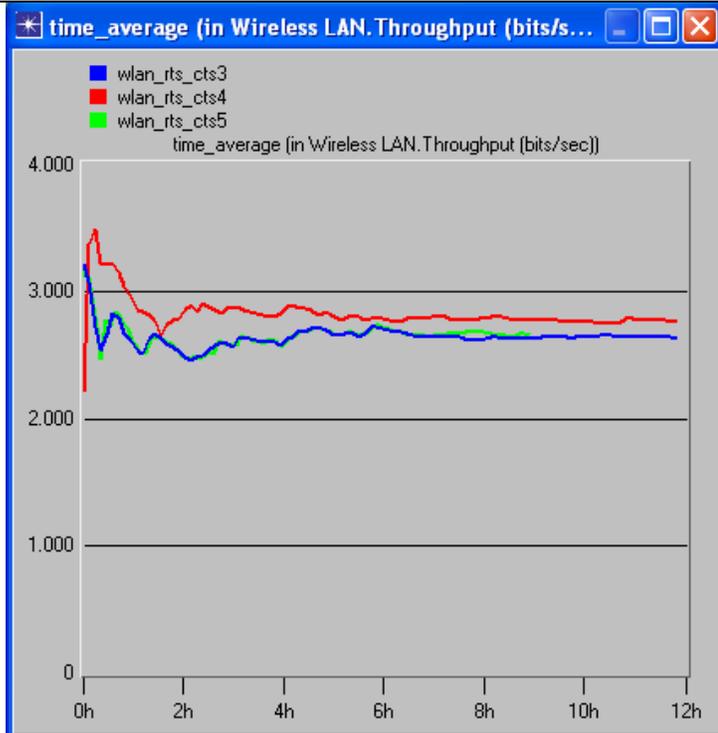


Fig 51. Comparación de datos recibidos.

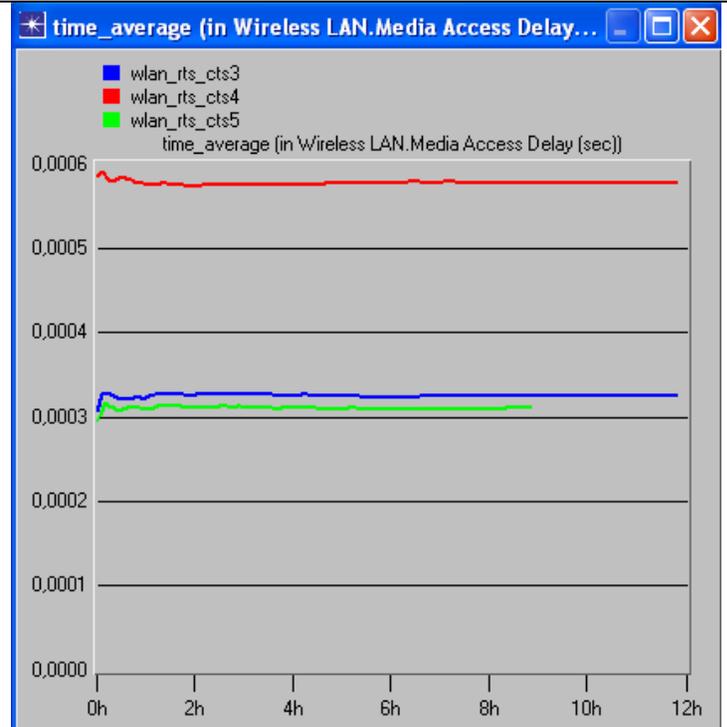


Fig 52. Comparación acceso al medio.

5.3.1 Análisis de resultados

Recordemos que existen dos formas de activar RTS / CTS, número uno, en las estaciones de trabajo y número dos, en el punto de acceso. Métodos a los cuales analizaremos ventajas y desventajas de acuerdo a las simulaciones y obtendremos conclusiones.

Para los dos casos realizamos unas simulaciones en la que verificamos el funcionamiento de RTS / CTS activado con tres posibles escenarios:

1. RTS Threshold = 2000.
2. RTS Threshold = 256.
3. RTS Threshold = Desactivado.

Recordemos que el método para habilitar RTS / CTS es colocar un tamaño de paquete específico denominado RTS Threshold que va de 0 a 2347 bytes. De acuerdo con esto, para un escenario con RTS / CTS activado en el punto de acceso, si el paquete que el punto de acceso trata de transmitir es mayor que el threshold, se iniciara la función RTS / CTS. Si el tamaño del paquete es igual o menor al threshold, el punto de acceso no activara RTS / CTS y enviara el paquete inmediatamente. El uso del threshold en 2347 bytes desactiva RTS / CTS para el punto de acceso.

Primero que todo observamos que para los escenarios *wlan_rts_cts 0,1 y 2* el acceso al medio de cada uno de los escenarios tuvo lugar en distintos intervalos de tiempo (Fig. 48), en el que particularmente observamos que al escenario *wlan_rts_cts 2* fue el que le tomo mas tiempo, lo que quiere decir que el mecanismo se activo y la red tuvo que lidiar con una trama mas larga de verificación para poder enviar los datos. Recordemos que al activar RTS / CTS en un equipo, este no enviara datos hasta que el equipo en espera complete el proceso RTS / CTS. Para todas las simulaciones con RTS / CTS activado, un

equipo inicia el proceso enviando una trama RTS. El equipo en espera recibe la trama RTS y responde con una trama CTS. El equipo que transmite debe recibir una trama CTS antes de enviar la trama de datos. La trama CTS también contiene un valor de tiempo que alerta a las otras estaciones que esperen para acceder al medio mientras la estación transmisora envía sus datos.

Al observar los paquetes enviados, paquetes recibidos y los datos perdidos (Figuras 46, 47 y 45, respectivamente) podemos decir que realmente no hay mucha diferencia en alguno de estos parámetros. Tener activado o desactivado el mecanismo en el punto de acceso no trae muchos beneficios.

De acuerdo a lo visto en las simulaciones podemos concluir que activar este mecanismo en una red que no presenta ningún problema, es decir en una red donde no hay pérdida de datos considerable, realmente no es un beneficio para la red. Tenga en mente que un incremento en el funcionamiento de la red usando RTS / CTS, es el resultado de introducir mas cabecera en la trama (overhead). Si usted no tiene ningún nodo oculto, entonces el uso de RTS / CTS solo incrementara la cantidad de "overhead" en la red. Usar RTS / CTS para solucionar un problema que no existe o un problema de nodo oculto muy pequeño (de 100 estaciones solo 1 presenta el problema), resultara en la degradación del funcionamiento de la red. En este caso, la trama adicional RTS / CTS hace mas daño introduciendo "overhead" que lo que se gana resolviendo el problema. Sea entonces cuidadoso al implementar RTS / CTS. Una de las mejores formas de determinar si usted debe activar RTS / CTS es monitoreando la WLAN para encontrar colisiones.

Iniciar RTS / CTS en el punto de acceso no tiene caso ya que el problema del nodo oculto no existe desde la perspectiva del punto de acceso. Forzar al punto de acceso a implementar RTS / CTS incrementara significativamente la cabecera de la trama (overhead) y reducirá los paquetes recibidos (Throughput), como se observo en la figuras 48 y 47, respectivamente. Por lo que solo queda una opcion:

concentrarse en usar RTS / CTS en las estaciones para mejorar el funcionamiento de la red.

Para poder observar el comportamiento de la red con RTS / CTS activado desde las estaciones los escenarios *wlan_rts_cts* 3,4 y 5 fueron creados.

Primero que todo debemos saber que para poder activar RTS / CTS en una estación en la "vida real", se debe configurar en las NICs (**Network interface cards o tarjetas de red de interfase**) de cada estación la opción de: *habilitar RTS / CTS*; se busco este parámetro en las opciones de los parámetros del simulador y se habilito en cada una de las estaciones el parámetro RTS Threshold de las redes locales inalámbricas. Una vez hecho esto se muestra el comportamiento de la red con RTS / CTS activado en las estaciones: el acceso al medio (Fig. 52) otra vez se ve seriamente afectado por este mecanismo, el escenario *wlan_rts_cts* 4 tiene más retraso en acceder al medio debido a que su trama de verificación es mas larga que la de los demás escenarios (*wlan_rts_cts* 3 y 5). También observamos que los paquetes enviados y recibidos (Figuras 50 y 51) presentan una pequeña mejora con el mecanismo activado y que los datos perdidos se mantienen casi iguales a través del tiempo (Fig. 49), por lo que podemos concluir que los beneficios obtenidos en los paquetes enviados y recibidos no justifican la demora de valor significativo que se presenta en el escenario con RTS / CTS activado. Por lo que se concluye también que activar este mecanismo en las estaciones en una red que no lo necesita conlleva a la degradación del funcionamiento de la red.

También podemos concluir que no es lo mismo tener el mecanismo activado y mandando datos inmediatamente, que no tenerlo activado del todo. Si observamos las figuras 48 y 52 podemos observar que en los escenarios *wlan_rts_cts* 2 y 5, el retraso de acceso al medio es menor que los escenarios *wlan_rts_cts* 0 y 3, debido a que en los escenarios *wlan_rts_cts* 0 y 3 aunque el paquete a enviar es menor que el Threshold especificado, de todas formas debe verificar que es

menor, lo cual conlleva de todas formas a que se demore un poco mas verificando la trama.

Para finalizar, tenga en cuenta que para activar RTS / CTS, se deben examinar cuidadosamente las colisiones, y una vez activado, se debe observar el desempeño de la red y estar absolutamente seguro de que el problema se soluciono sin disminuir el desempeño, después de todo, el objetivo es mejorar el funcionamiento de la red.

5.4 WLAN CON PUNTO DE ACCESO.

Recordemos que este escenario consiste en la interconexión de una red inalámbrica y una red cableada mediante el backbone de Internet.

Para poder resaltar las características de una LAN wireless por medio del backbone de Internet, conectada a la misma por medio de un punto de acceso debemos crear dos escenarios: uno que identifique el comportamiento de la WLAN con las características especificadas y otro escenario que consiste en una red LAN Ethernet cableada también conectada a través del backbone de Internet, con el objetivo de comparar las redes, establecer diferencias o semejanzas y obtener conclusiones.

El primer paso es crear un escenario y lo llamamos: **wlan_access_point**. Para este escenario crearemos dos redes:

1. Una es una red con estaciones inalámbricas conectándolas a un servidor por medio del backbone de Internet.
2. Y la otra es una red totalmente cableada, con sus estaciones también conectadas a un servidor, cableadas por medio del backbone de Internet.

Para la primera red seleccionamos los siguientes equipos de la paleta de objetos y los colocamos en el área de trabajo:

Cantidad	Tipo	Grafico
2	subnet	
1	ethernet4_slip8_cloud	
1	Application config	
1	Profile config	
5	Wlan_wkstn_adv(fix)	
1	Wlan_ethernet_router_adv (fix)	
1	Ethernet_server_adv	
1	Ethernet2_slip8_gtwy_adv	

Tabla 8. Equipos para *wlan_access_point* red No1.

Colocamos las dos subredes, la aplicación, el perfil y la nube IP, debemos ver una grafica como esta:

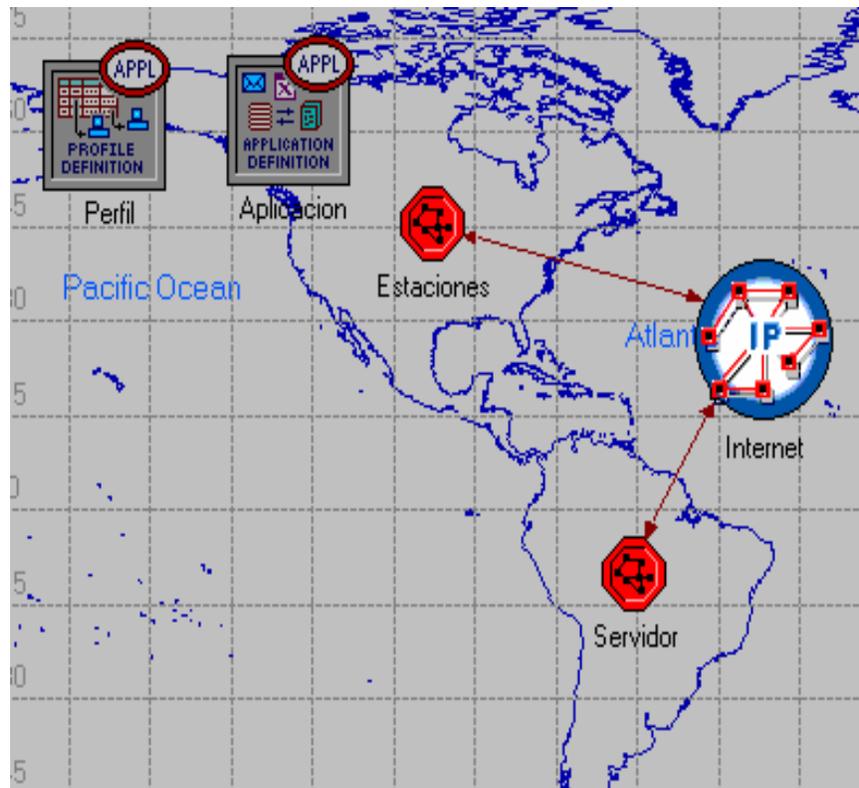


Figura 53. Subredes y nube IP colocadas en el escenario *wlan_access_point*.

Nombramos a las dos subredes: Estaciones y servidor, respectivamente, y para la nube IP realizamos la siguiente configuración:

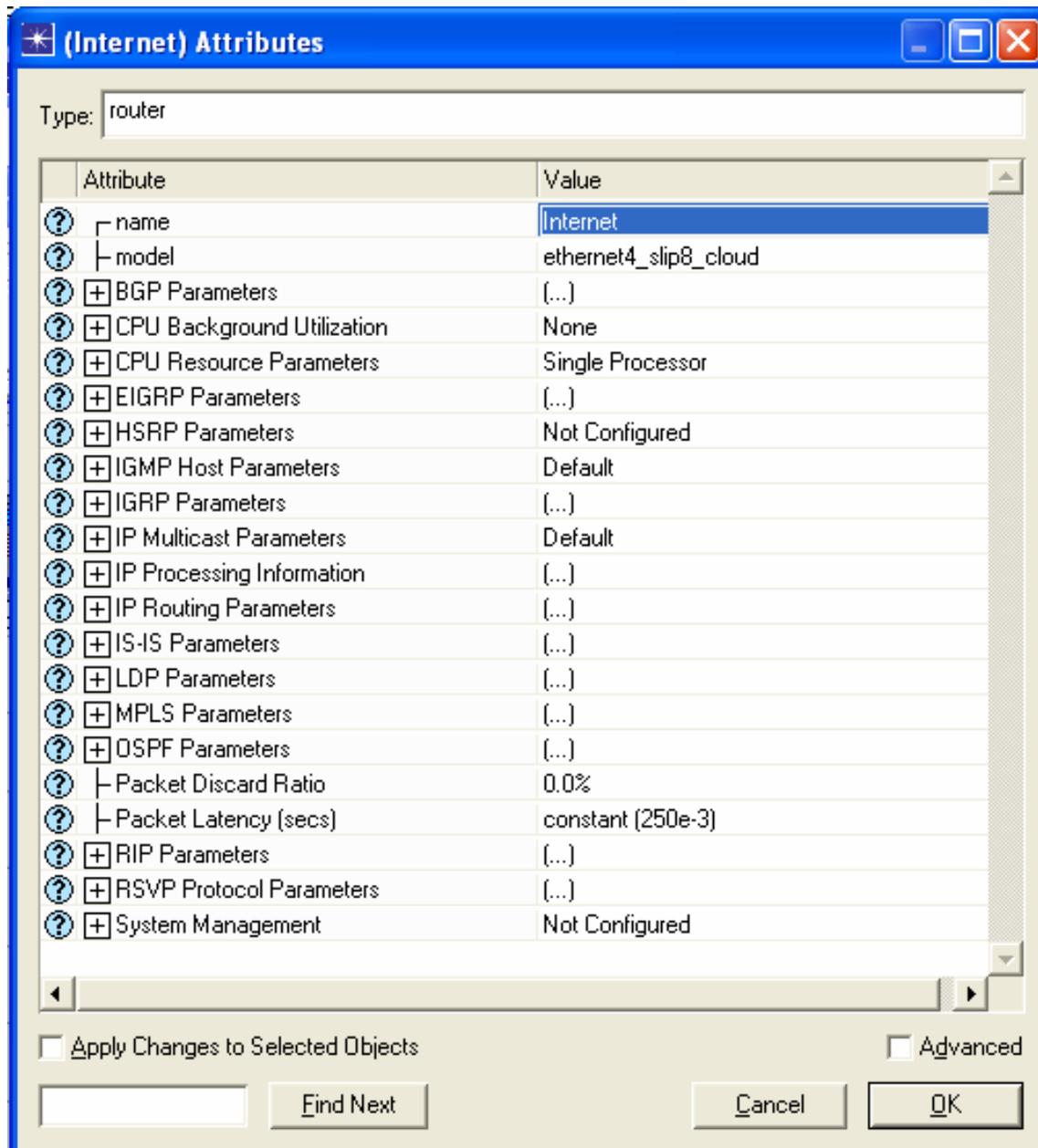


Figura 54. Configuración de atributos de la nube IP.

Es muy importante definir y configurar correctamente las aplicaciones que se van a ejecutar en la red. El comportamiento de un usuario o su perfil puede ser descrito por las aplicaciones que utiliza, por el tiempo que las utiliza o por cuan a menudo utiliza esas aplicaciones en el día. Un número de aplicaciones comunes de red como ser e-mail, telnet, base de datos, http han sido desarrolladas en OPNET para su simulación. El objeto **Application Definition** ubicado en la paleta de objetos es el encargado de configurar dichas aplicaciones y el objeto **Profile Definition** es el encargado de describir los patrones de actividad de un usuario en la red.

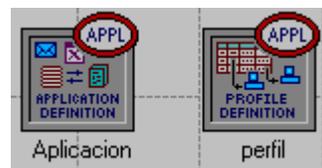


Figura 55. Definición de la aplicación y el perfil.

Seleccionamos estos ítems de la paleta de objetos y los arrastramos al área de trabajo. Hacemos clic derecho en el objeto **Application Definition**, hacemos clic izquierdo en *Edit_Attributes* y configuramos los siguientes parámetros:

1. Cambiamos el nombre del objeto **Application Definition**, haciendo clic en **Name**, colocamos: *Aplicación*.
2. Hacemos clic en **Application_Definitions** > creamos un nuevo vector en **row**, lo cual dará la opción para la creación de aplicaciones existentes y una opción especial para que el usuario cree la aplicación de su gusto.
3. Seleccionamos **Description** > **Ftp** > **Edit**.
4. Modificamos el tamaño del paquete en **File_Size** a **exponential (1024)**.
5. Clic **OK**.
6. Para finalizar modificamos el nombre de la aplicación en el parámetro **Name** que se encuentra en el vector, colocamos: *Ftp aplicación*.
7. Clic **OK**.

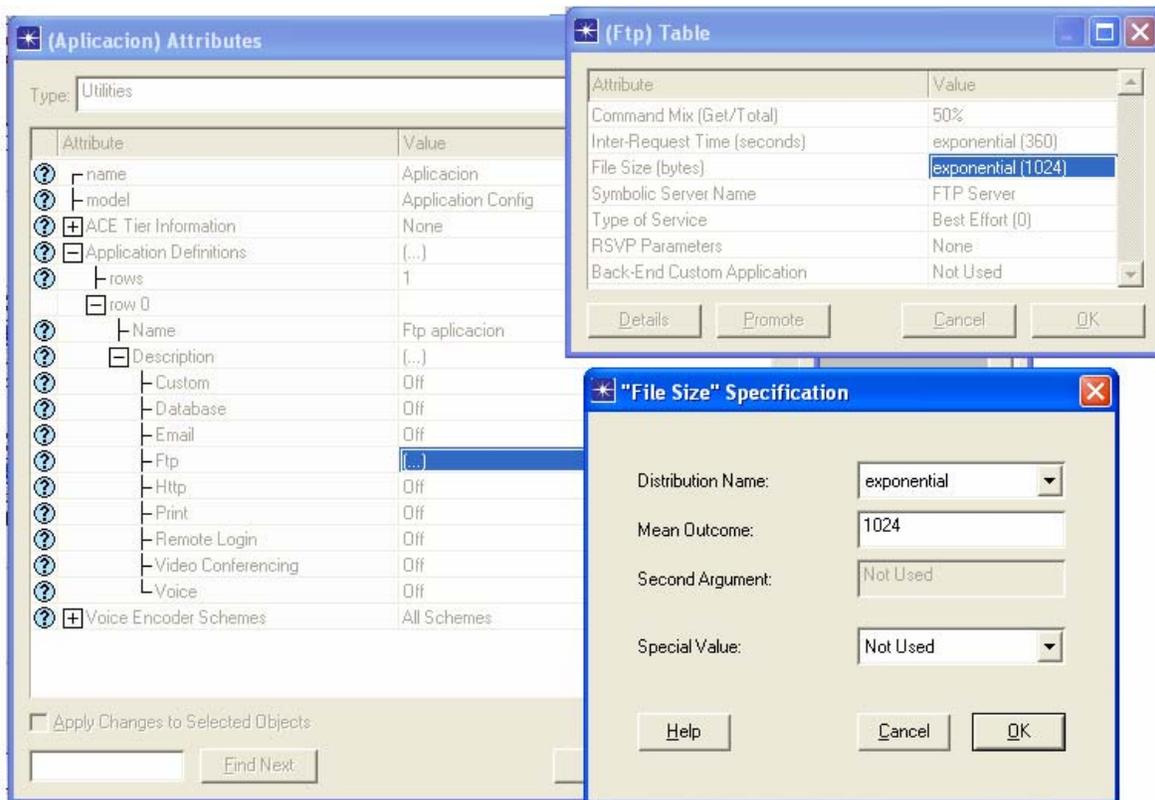


Figura 56. Ventanas de configuración de la aplicación.

Procedemos ahora a modificar los parámetros del perfil seleccionándolo con clic derecho y luego haciendo clic izquierdo para elegir *Edit_Attributes*:

1. Cambiamos el nombre del objeto **Profile_Definition** haciendo clic en **Name**, colocamos: *Perfil*.
2. Hacemos clic en **Profile_Configuration** > creamos un nuevo vector en **row** > seleccionamos **Application** para elegir la aplicación del perfil > seleccionamos **Edit** y en la tabla creamos un nuevo vector y seleccionamos la aplicación previamente creada.
3. Clic **OK**.
4. Para finalizar modificamos el nombre del perfil en el parámetro **Profile_Name**, colocamos: *Ftp perfil*.
5. Clic **OK**.

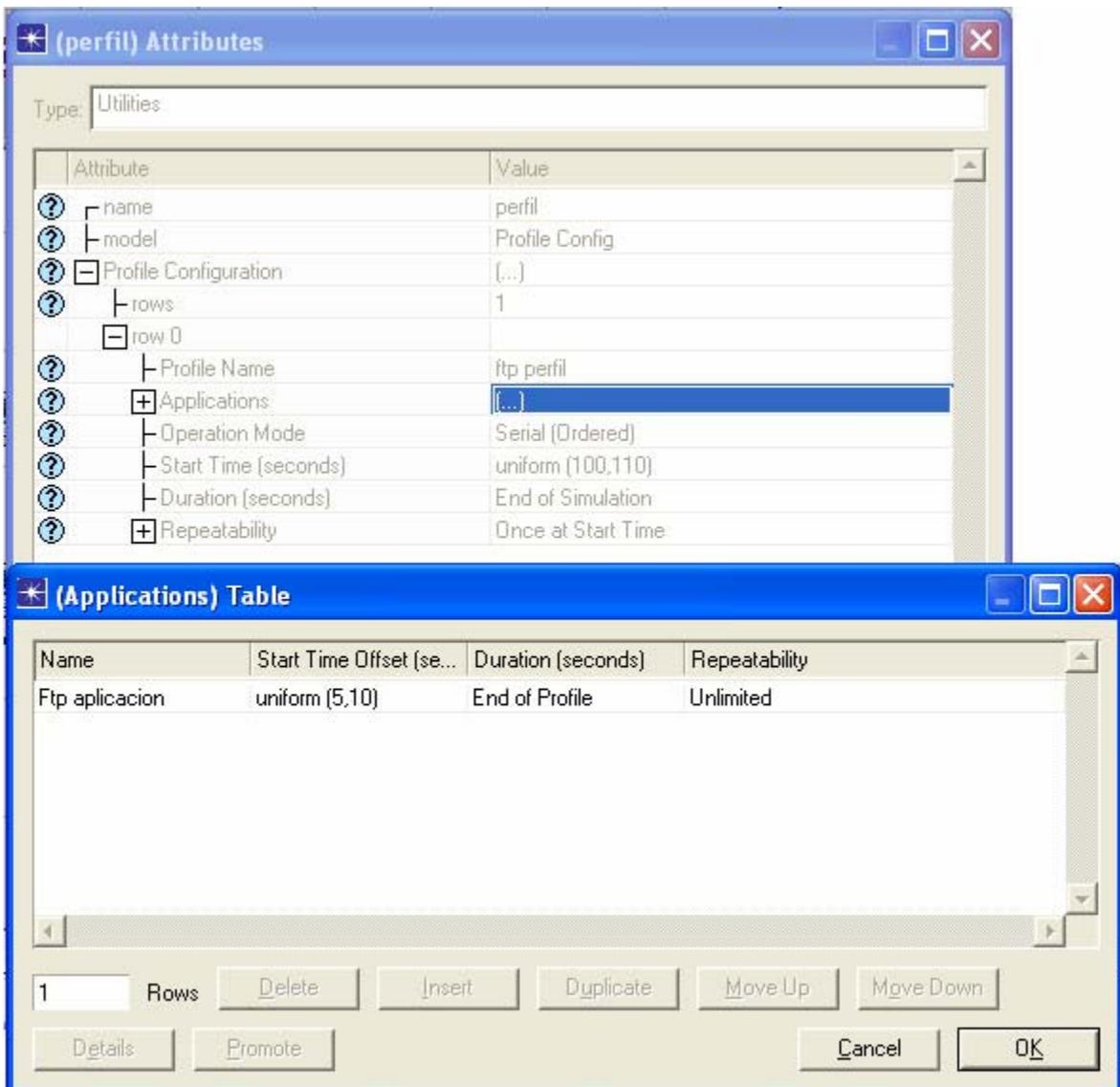


Figura 57. Ventanas de configuración del perfil.

NOTA: elegimos la aplicación *Ftp* debido a que esta es una aplicación que permite la transferencia de archivos entre un cliente y un servidor, ideal debido a que se encuentra en todo tipo de redes.

Para poder configurar la aplicación y el perfil bajo FTP en el servidor y en las estaciones respectivamente, proseguimos de la siguiente forma:

1. En el servidor modificamos el parámetro **Application Supported Services** >seleccionamos **Edit** > creamos un vector y seleccionamos la aplicación **Ftp aplicación** > Clic **OK**.
2. En las estaciones seleccionamos el parámetro **Application Supported Profiles** >seleccionamos **Edit** > creamos un vector y seleccionamos **Ftp perfil** > Clic **OK**.

Proseguimos con la configuración de las subredes haciendo doble clic en la subred: estaciones. Aquí colocamos las 5 estaciones inalámbricas y el router inalámbrico. Para las estaciones acuérdesese de asignar el perfil de FTP y una velocidad de transmisión (**Data Rate**) de 11Mbps.

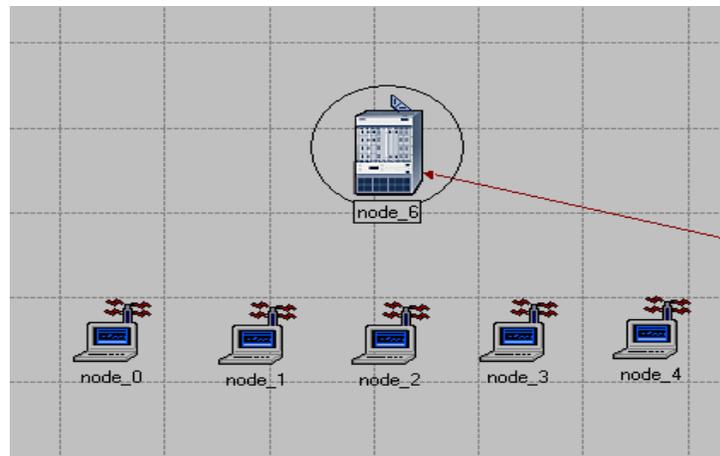


Figura 58. Equipos en la subred *estaciones* de *wlan_access_point* red No1.

Nuevamente hacemos doble clic, pero ahora en la subred: servidor. Colocamos el router y el servidor ethernet. No se olvide de asignar la aplicación al servidor.

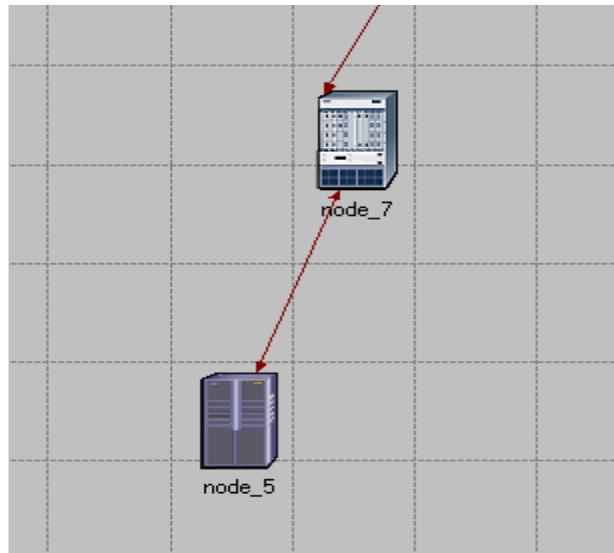


Figura 59. Equipos en la subred *servidor* de *wlan_access_point* red No1.

Cableamos los equipos y la nube IP de acuerdo a la siguiente tabla:

Nodo	Nodo	Cableado
		 100BaseT_adv
		 1000BaseX_adv
		 1000BaseX_adv

Tabla 9. Cableado de equipos en *wlan_access_point*.

Para realizar una red ethernet típica seleccionamos los siguientes elementos:

Cantidad	Tipo	Grafico
2	subnet	
1	ethernet4_slip8_cloud	
5	ethernet_wkstn_adv	
1	Ethernet8_switch_adv	
2	Ethernet2_slip8_gtwy_adv	
1	Ethernet_server_adv	

Tabla 10. Equipos para *wlan_access_point* red No2.

Nombramos las dos subredes y la nube IP: Estaciones_0, servidor_0 e Internet_0, respectivamente. Colocamos los items sobre la misma área de trabajo de la primera red:

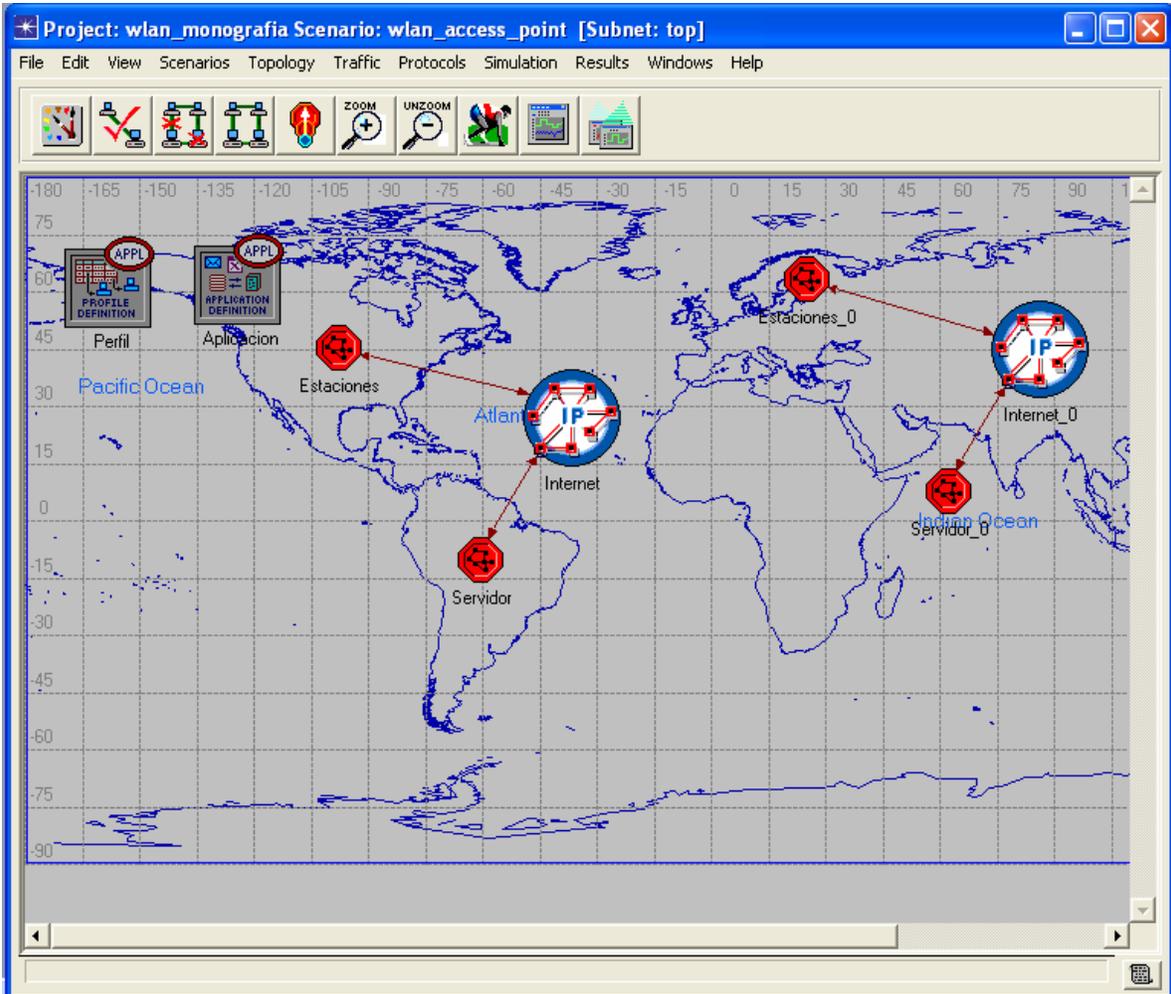


Figura 60. Vista general escenario *wlan_access_point*.

Hacemos doble clic en la subred: estaciones_0. Aquí colocamos las 5 estaciones, el switch y el router ethernet. Para las estaciones acuérdesese de asignar el perfil de FTP.

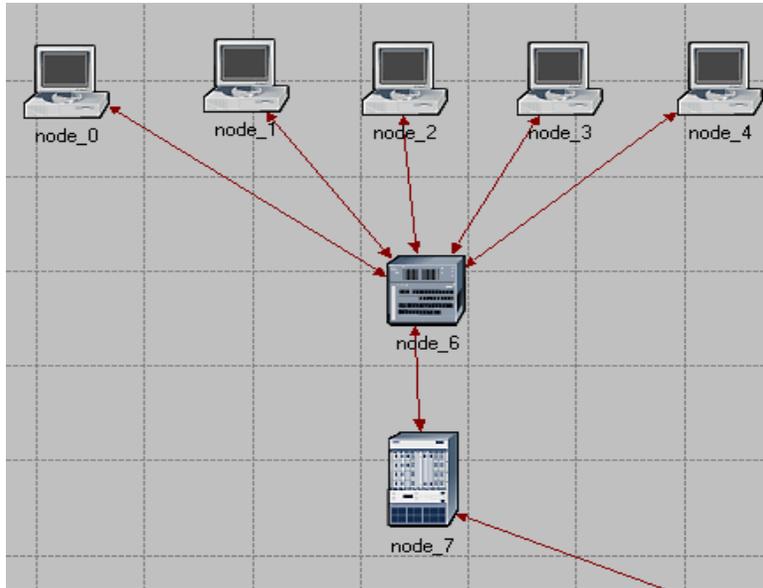


Figura 61. Equipos en la subred *estaciones_0* de *wlan_access_point* red No2.

Nuevamente hacemos doble clic, pero ahora en la subred: servidor_0. Colocamos el router restante y el servidor ethernet. No se olvide de asignar la aplicación al servidor.

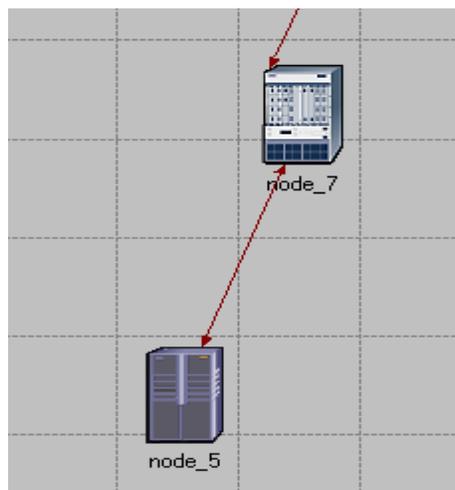


Figura 62. Equipos en la subred *servidor_0* de *wlan_access_point* red No2.

Cableamos la red de acuerdo a la siguiente tabla:

Nodo	Nodo	Cableado
		 100BaseT_adv
		 1000BaseX_adv
		 100BaseT_adv
		 10BaseT_adv

Tabla 11. Cableado de equipos en *wlan_access_point* red No2.

Para poder obtener conclusiones elegimos las siguientes estadísticas:

Escenario	Parámetros	
	<i>Global Statistics</i>	<i>Node Statistics</i>
<i>Wlan_access_point</i>	<i>Wireless LAN > Todas</i>	<i>Ethernet > Load (bits/sec)</i>
	<i>Ethernet > Todas</i>	<i>Ethernet > Traffic Received (bits/sec)</i>
		<i>Ethernet > Delay</i>
		<i>Wireless LAN > todas</i>

Tabla 12. Estadísticas de *wlan_access_point*.

Corremos la simulación por 60 minutos para analizar el comportamiento de la red y obtener conclusiones. Vamos a **view results** y obtenemos los siguientes resultados:

1. Load Red con punto de acceso (azul) Vs Red totalmente cableada (roja)

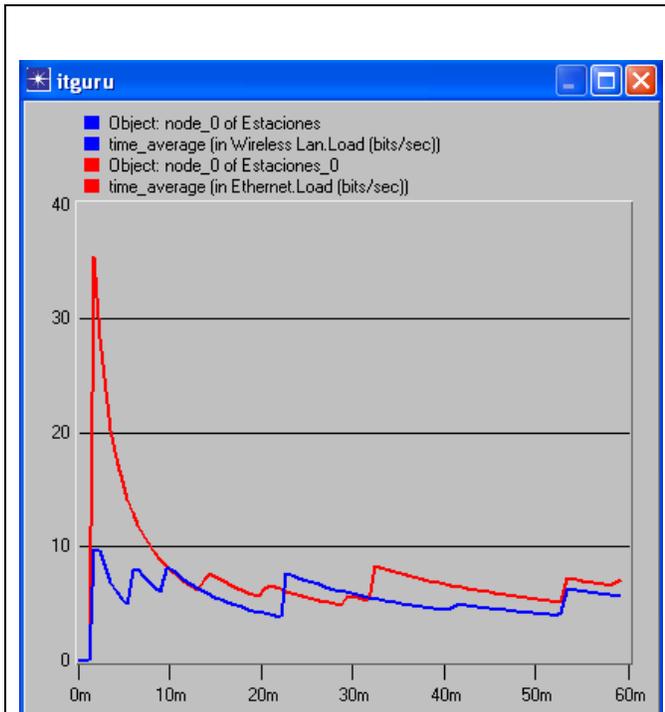


Fig 63. Comparación Load nodo 0.

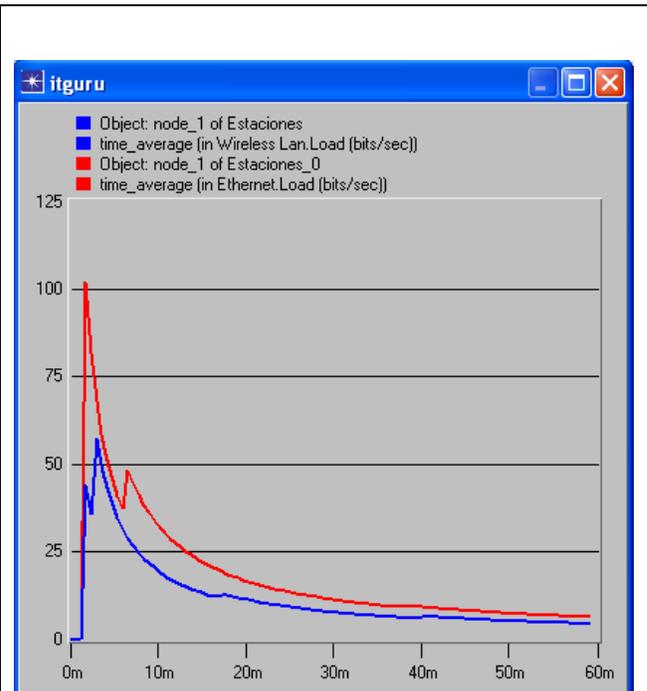


Fig 64. Comparación Load nodo 1.

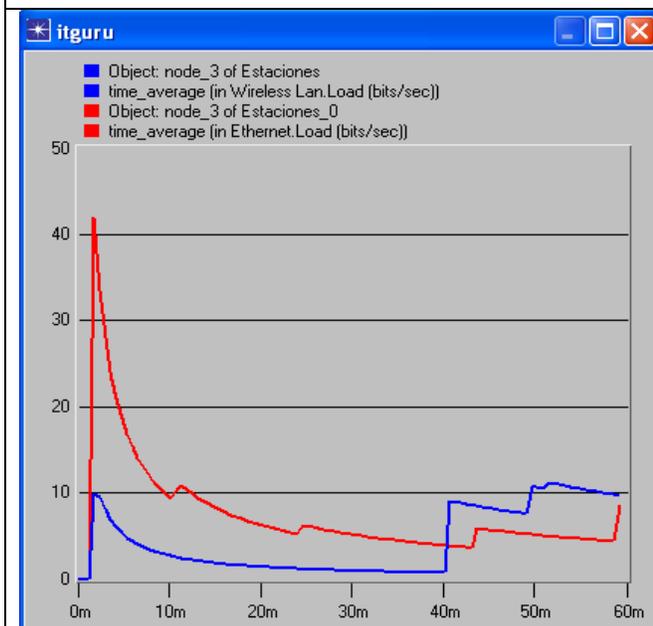


Fig 65. Comparación Load nodo 3.

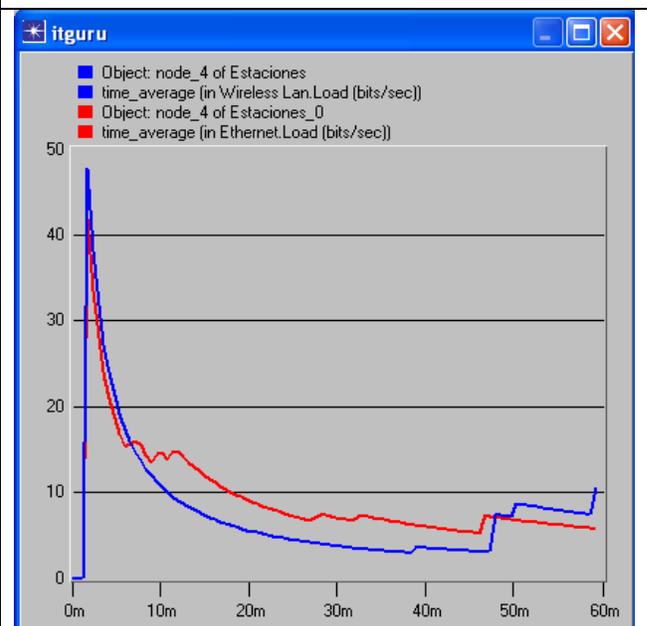


Fig 66. Comparación Load nodo 4.

2. Throughput Red con punto de acceso (azul) Vs Red totalmente cableada (roja)

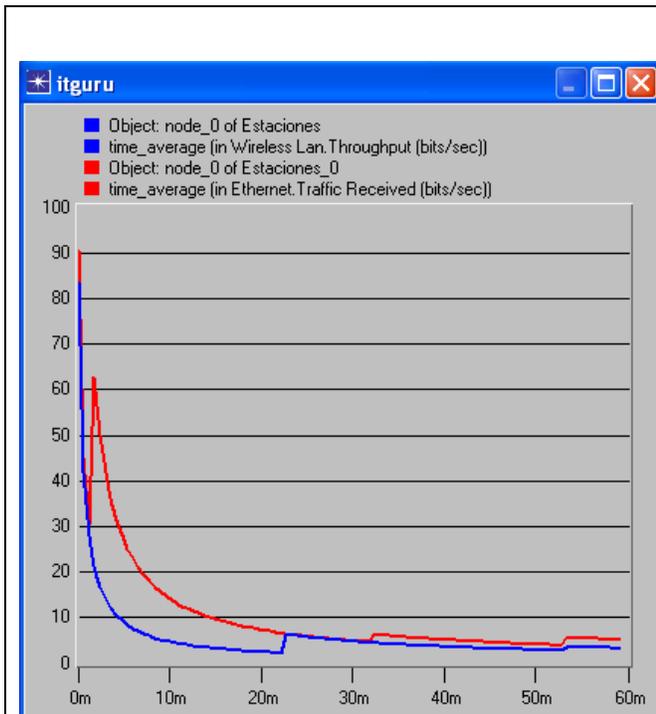


Fig 67. Comparación Throughput nodo 0.

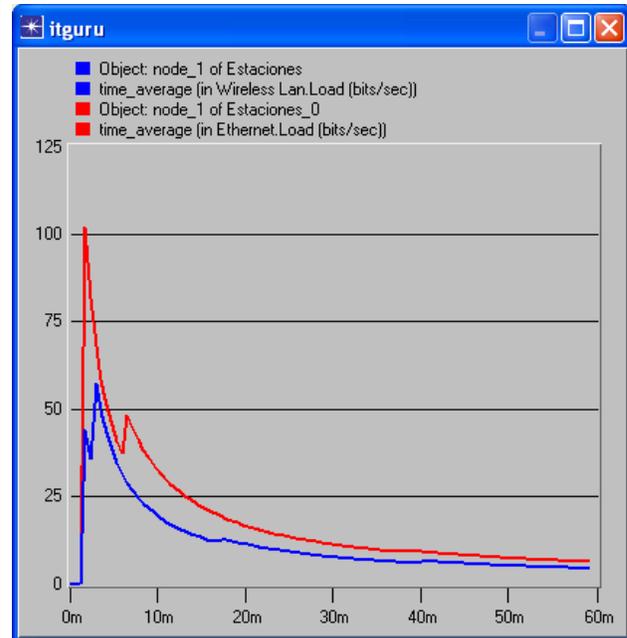


Fig 68. Comparación Throughput nodo 1.

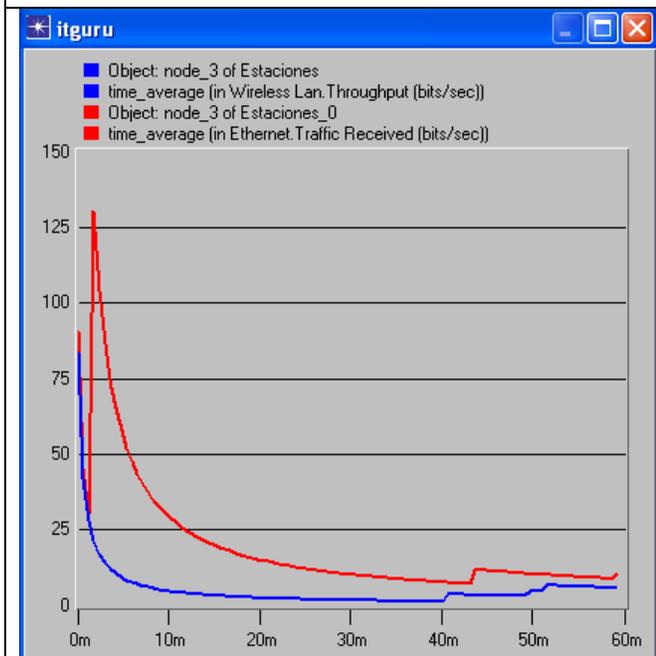


Fig 69. Comparación Throughput nodo 3.

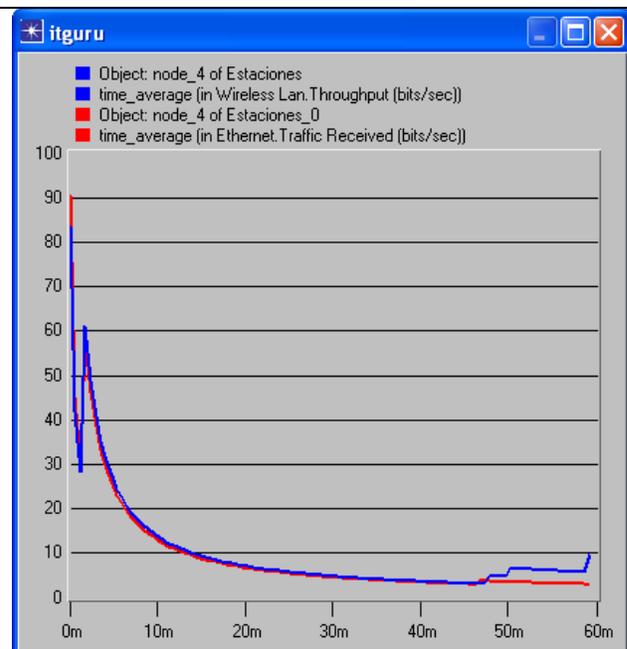


Fig 70. Comparación Throughput nodo 4.

3. Delay de una Red con punto de acceso (azul) Vs Delay de una Red Ethernet (roja)

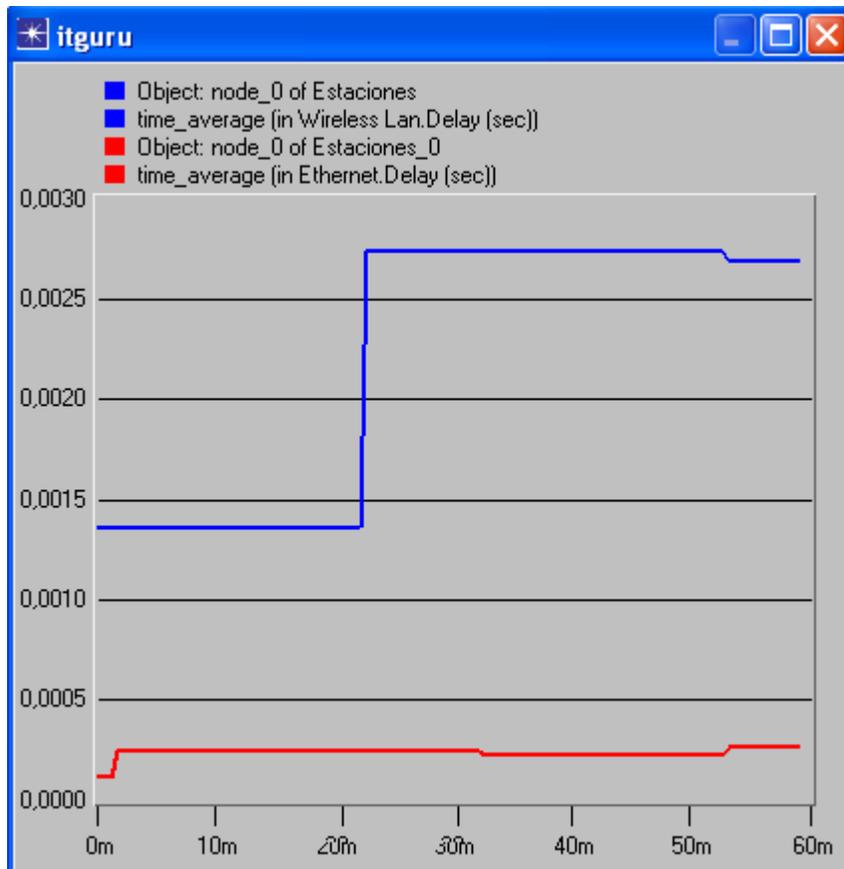


Fig 71. Comparación del Delay nodo_0 de una red con punto de acceso (azul) Vs Delay nodo_0 de una red Ethernet (roja)

5.4.1 Análisis de resultados

El método de acceso de una WLAN es CSMA/CA donde CA significa evasión de colisiones (*Collision Avoidance*). Note que eso no es lo mismo que CSMA/CD, en donde CD traduce: detección de colisiones, que es el método utilizado por una LAN cableada ethernet. En CSMA/CD se les garantiza a todos los clientes escuchar las transmisiones de otros clientes, mientras que con CSMA/CA no es posible para todos los clientes escuchar la transmisión de los demás en todo

momento. En las redes inalámbricas, por lo tanto no se puede escuchar a la vez que se transmite: no pueden detectarse colisiones, por lo que deben existir mecanismos para evitarlas. Esto conlleva a que el procesamiento de los datos en una red inalámbrica sea mas lento que el de una red totalmente cableada (Fig. 71), la red inalámbrica debe correr mecanismos de prevención que eviten estas colisiones y de esta forma transmitir los datos de forma óptima.

Tales mecanismos adhieren más cabecera (overhead) y reducen los paquetes recibidos y enviados en un 50 - 60% en comparación con una red cableada, si observamos las figuras de la 63 a la 70 nos podemos dar cuenta de esto, solo que en el nodo 4 se presenta una excepción: los paquetes enviados y recibidos son casi iguales; por lo que también podemos concluir que para casos excepcionales un nodo de cada cinco puede poseer las características de recepción y transmisión de la calidad de una red cableada, lo cual no es ideal para una red, imagínese una red donde se anuncie que todos los nodos tienen velocidades de transmisión y recepción bajas pero le aseguran que una va ser buena, lo ideal es que todos los nodos de la red, beneficien la red. Concluimos que una WLAN sencilla con un punto de acceso es como una radio de pulso para hablar, su método de transmisión es half-duplex, por lo que se considera en este sentido que es igual a un hub de una LAN cableada, donde todas las estaciones deben escuchar otras transmisiones y todas competir por acceder al medio compartido.

Las WLANs poseen métodos de comunicación Half- duplex, medios de transmisión compartidos y velocidades más lentas que las redes cableadas, solo basta con mirar la figura 71 para darse cuenta que el retraso de los paquetes en una WLAN es mayor que en una LAN cableada. Cuando se abandona el cable se gana libertad de movimiento pero se pierde al mismo tiempo funcionalidad de la red.

Cuando observamos bien la naturaleza hub de una WLAN, llegamos a la conclusión de que un punto de acceso no es más que una combinación de un

puente (bridge) de dos puertos con un hub inalámbrico conectado a uno de sus puertos.

Por lo tanto usted debe analizar de manera cuidadosa al instalar una red WLAN, debe observar si los parámetros de la WLAN cumplen con los objetivos de la red, ya que si escoge de manera rápida sin analizar la situación cuidadosamente puede que este perdiendo su dinero de manera anticipada.

Los resultados obtenidos en este escenario parecen devastadores para las redes inalámbricas, pero no seamos tan pesimistas, la verdad es que los equipos actuales como los WLAN router, swicht, entre otros, satisfacen las necesidades más básicas o estándar del usuario: acceso de archivos, impresoras y aplicaciones de servidor. Además las redes WLAN todavía están evolucionando, y a pesar de sus problemas poseen ventajas grandes como la movilidad: la oportunidad de acceder a la información desde cualquier punto sin necesidad de la conexión física al puerto permite un gran ahorro de tiempo y productividad, y su fácil expansión, ya que solo es posible agregar equipos a la red sin la necesidad de comprar cables y trazar rutas.

5.5 WLAN SWITCHED y ROUTED

Con el objetivo de entender mejor estos dos escenarios, nos pareció conveniente analizar estos escenarios juntos, para así analizar como se comportan estos medios de comunicación ante los mismos parámetros y obtener conclusiones en base a los resultados.

Para este escenario debemos crear dos escenarios: *wlan_router* y *wlan_switch*. Para los dos escenarios observamos como se comporta la WLAN con cada uno de estos equipos, por lo que es de suma importancia seleccionar los parámetros del comportamiento de la WLAN global (***Global Statistics***).

Para wlan_router y switch debemos seleccionar de la paleta de objetos los siguientes elementos:

Cantidad	Tipo	Grafico
5	subnet	
1	1000BaseX_adv	
1	Application config	
1	Profile config	
20	Wlan_wkstn_adv(fix)	
4	Wlan_ethernet_router_adv (fix)	
1	Eth4_slip4_multihomed_server_adv	
20	Wlan_station_adv (fix)	
4	Wlan_eth_bridge_adv	

Tabla 13. Equipos de wlan_router y switch.

NOTA: Se eligió este servidor debido a que era el único que soportaba la interconexión directa de 4 equipos tecnología ethernet, perfecto para probar los equipos inalámbricos sin equipos intermedios que puedan afectar el campo de medición o la respuesta de los mismos.

Realizamos la interconexión de las redes como se muestra a continuación:

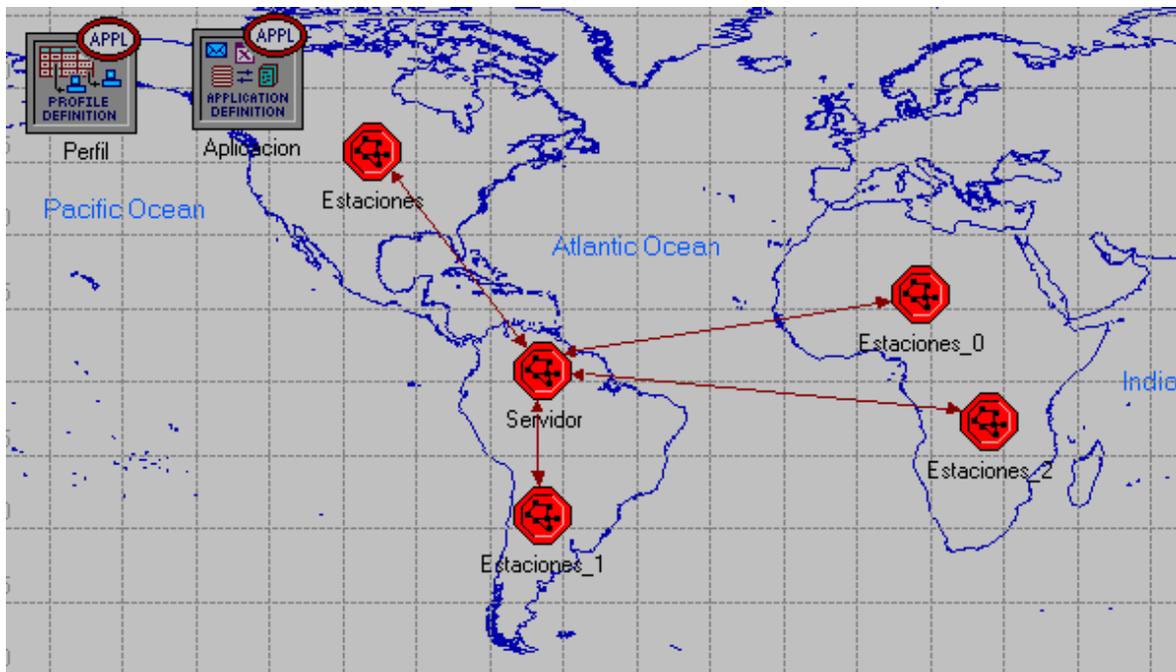


Figura 72. Vista general para los escenarios *wlan_router* y *switch*.

En cada red de estaciones para *wlan_router*, tendremos la siguiente configuración de equipos:

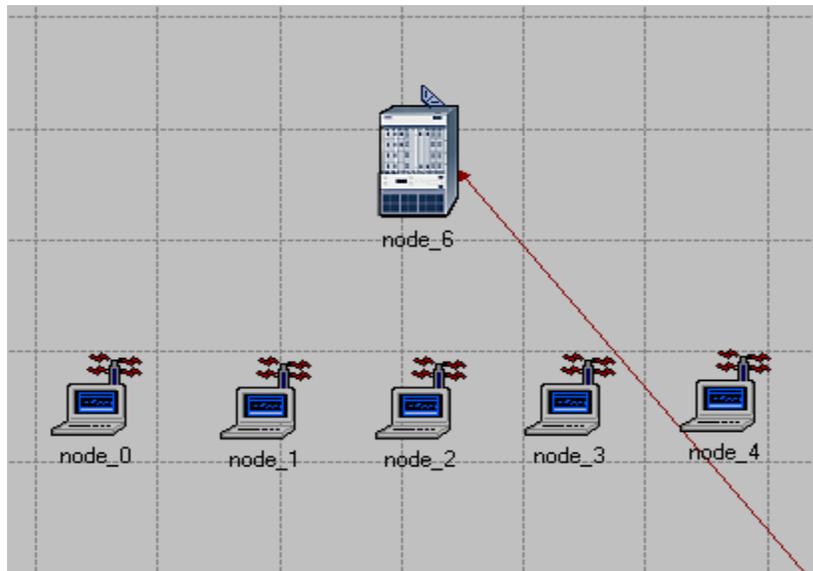


Figura 73. Equipos para las subredes de estaciones de *wlan_router*.

En cada red de estaciones para *wlan_switch*, tendremos la siguiente configuración de equipos:

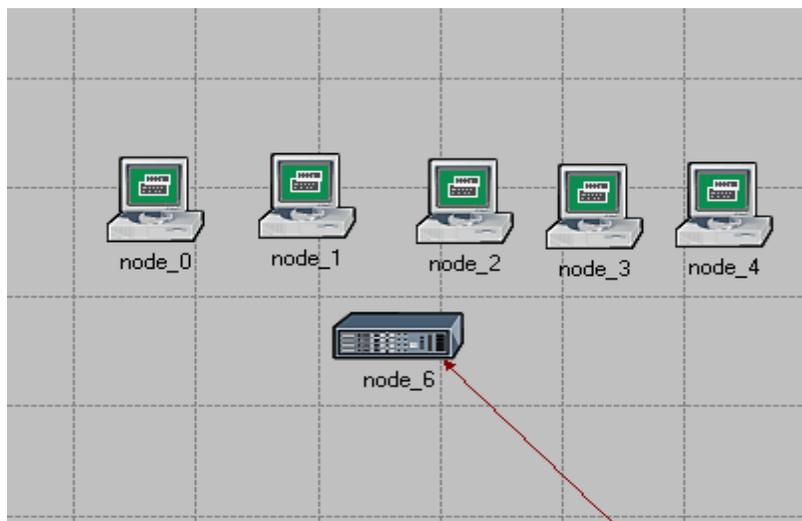


Figura 74. Equipos para las subredes de estaciones de *wlan_switch*.

En la red del servidor para *wlan_router* y *wlan_switch*, tendremos la siguiente configuración de equipos:

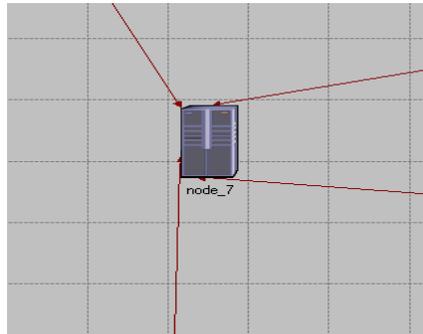


Figura 75. Equipos para la subred de servidor de *wlan_router* y *switch*.

NOTA: Los enlaces entre equipos se realizaron todos con el mismo link. Recuerde que son dos escenarios completamente diferentes: *wlan_router* y *wlan_switch*.

Configuramos los parámetros de los equipos de la siguiente forma:

Escenario	Parámetros		
Wlan_router	Servidor	Access Point	Estaciones
	Wireless LAN Parameters		
	Application supported services = ftp_aplicacion	Data rate (bps) = 11 Mbps	Data rate (bps) = 11 Mbps
	-----	Access point functionality = enabled	Application supported profiles = ftp_perfil
Wlan_switch	Wireless LAN Parameters		
	-----	Data rate (bps) = 11 Mbps	Data rate (bps) = 11 Mbps
	-----	Access point functionality = enabled	-----
	Traffic generation parameters		
	-----	-----	Star time (sec) = constant (2)

Tabla 14. Configuración de los atributos de los equipos en *Wlan_switch* y *router*.

Comparamos los escenarios y obtenemos los siguientes resultados:

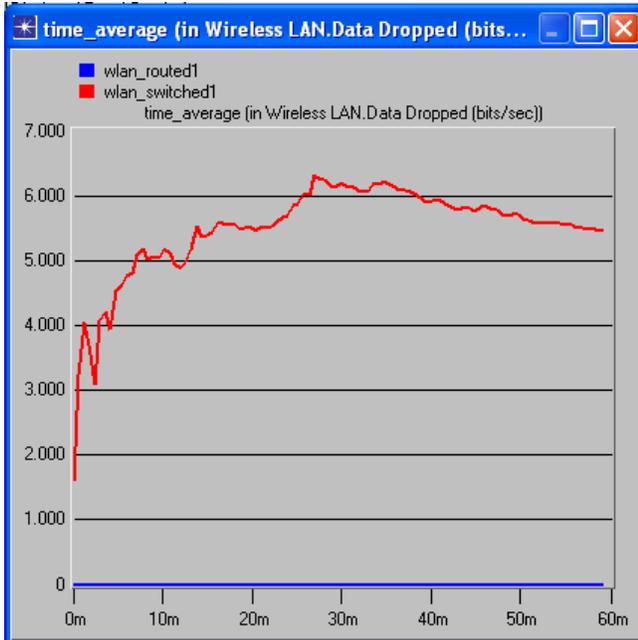


Fig 76. Comparación Data dropped de la WLAN.

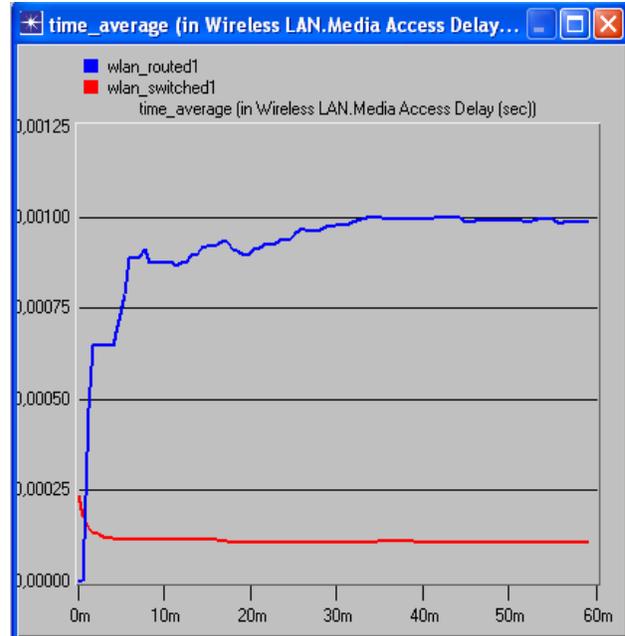


Fig 77. Comparación media access delay WLAN.

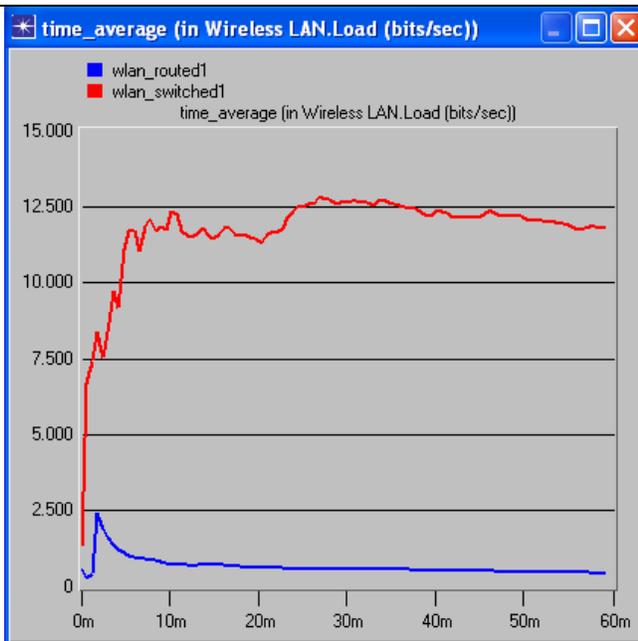


Fig 78. Comparación Load de la WLAN.

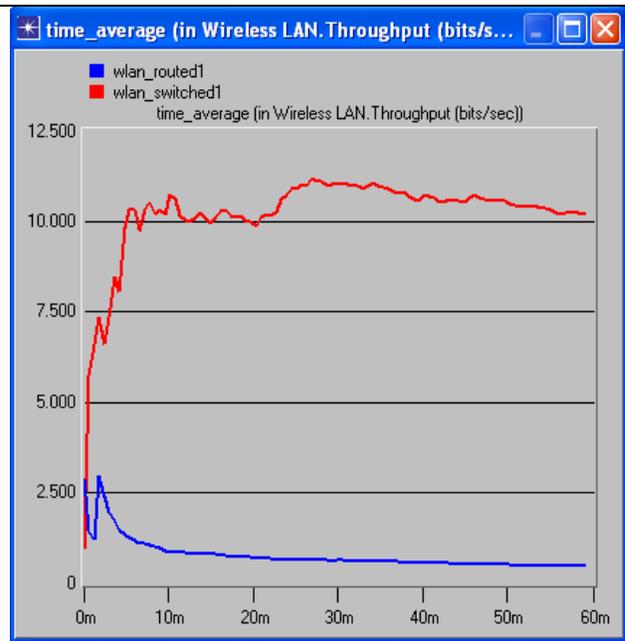


Fig 79. Comparación Throughput WLAN.

5.5.1 Análisis de resultados

La diferencia fundamental entre un switch y un router es que el switch opera en la capa 2 del modelo OSI y el router opera en la capa 3. Esta diferencia afecta la forma en que los switches y los routers responden al tráfico de la red. Lo cual podemos comprobar con tan solo mirar el tipo de estación que se utilizó para cada escenario. Para *wlan_router* fue necesario utilizar estaciones que soportaran aplicaciones, mientras que para *wlan_switch* se utilizaron estaciones que trabajan al nivel de la capa de enlace de datos.

Observando las gráficas de Throughput y load (figuras 79 y 78), podríamos decir que de acuerdo a los resultados, una red WLAN con un switch funciona mucho mejor que una con un router, ya que el valor de los paquetes enviados y recibidos es mayor. Pero OJO, no todos son paquetes, los LAN switches no filtran broadcast, multicast o tramas de dirección desconocida. La falta de filtrado introduce un serio problema: los broadcast que se originan de cada segmento son recibidos por todas y cada una de las estaciones en la red switchheada, lo que significa que grandes cantidades de ancho de banda se desperdicia por la transmisión de los mismos. La circulación de broadcast satura la red resultando en falta de ancho de banda para los datos importantes de la aplicación. En este caso, no se pueden implementar nuevas conexiones en la red, y las conexiones existentes pueden fallar (una situación conocida como broadcast storm, tormenta de difusión). La probabilidad de las tormentas de difusión incrementa a medida que la red switchheada crece. En contraste los routers no permiten los broadcast, y por lo tanto, no están sujetos a tormentas de difusión.

Las redes switchheadas de una LAN operan en la capa 2 del modelo OSI y tienen que proveer de conectividad a los usuarios como si cada uno de ellos estuviera en el mismo cable. Las direcciones de la capa 2 asumen un direccionamiento igualitario. En cambio, los routers trabajan en la capa 3 de OSI, por lo que ellos pueden formular e implementar una estructura de direccionamiento jerárquico. Los routers pueden asociar un direccionamiento del tipo lógico a una infraestructura física. El flujo del tráfico en una red routeada es muy diferente al flujo de una red

switchheada. Las redes con routers poseen un flujo de tráfico más flexible porque ellos pueden usar jerarquías para determinar caminos óptimos basados en factores como la congestión de la red. Basta con observar la figura 76, para observar como una red switchheada presenta más problemas de datos perdidos que una red routeada por problemas como la congestión de la red debido a tormentas de difusión, entre otros. La conclusión anterior nos hace reflexionar sobre la red switchheada: esta red no solo presenta mas paquetes enviados y recibidos debido a factores como broadcast, este comportamiento también se presenta debido a la cantidad de retransmisiones que deben hacer las estaciones de cada subred.

De la figura 77 se puede observar que el escenario *wlan_switch* tiene un mejor acceso al medio, pero recuerde que el escenario *wlan_routed* trabaja en la capa 3 del modelo OSI, este debe verificar y procesar una cantidad de protocolos inherentes a esta capa que lo caracterizan, cosa que no hace el escenario *wlan:switch*, que verifica protocolos mas rápidos que se encuentran en la capa 2.

De acuerdo a los resultados obtenidos, podemos concluir que un WLAN switch se comporta básicamente como un punto de acceso común y corriente: permiten a los clientes inalámbricos acceder a una red en particular sin traer muchos beneficios a la misma. Lo cual en contraste con un WLAN router, se observa que este le permite a los clientes dirigirse a un gran número de redes, como conectarse a Internet, entre otros servicios. El WLAN router siempre toma las direcciones IP y toma decisiones de cómo direccionar el paquete, en cambio los puntos de acceso ignoran la dirección IP y transitan todos los paquetes. Además los WLAN routers debido a que son mas inteligentes tienen la habilidad de proveer un mejor control de flujo, implementación de firewalls para no permitir mensajes indeseados, y entre otros servicios que lo hacen mucho mas versátil y lo diferencian del punto de acceso o de un WLAN swicht.

5.6 WLAN PCF

Recordemos que el modo PCF (Punto de coordinación de funciones) es un mecanismo alternativo para configurar el acceso al medio de cada una de los nodos de una red inalámbrica. Para comprobar las características del modo PCF, necesitamos un escenario WLAN que consta de unas estaciones inalámbricas y un punto de acceso, en donde se compruebe nuevamente verificación de las dos primeras capas del modelo OSI.

Para los dos escenarios tendremos los siguientes ítems de la paleta de objetos en el área de trabajo:

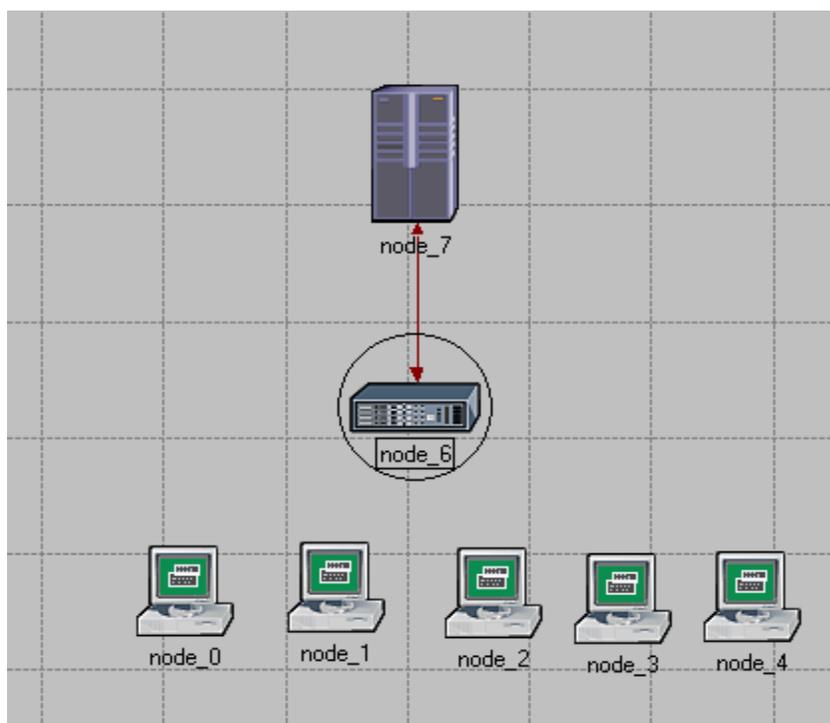


Figura 80. Equipos de escenarios *wlan_access_point_PCF* y *wlan_PCF*.

NOTA: los equipos seleccionados son los mismos con los que se ha estado trabajando durante todo el documento: *wlan_wksth_adv*, *Wlan_ethernet_bridge_adv* (fix) y *un servidor ethernet*..

Configuramos los atributos de los equipos de la siguiente forma:

Escenario	Parámetros	
Wlan_access_point_PCF	Access Point	Estaciones
	Wireless LAN Parameters	
	AP.functionality=enabled	Data rate = 11Mbps
	Data rate = 11Mbps	-----
Wlan_PCF	Wireless LAN Parameters	
	AP.functionality=enabled	Data rate = 11Mbps
	Data rate = 11Mbps	-----
	PCF parameters	
	PCF functionality = enabled	-----
	CFP Beacon multiple =1	-----
	CFP Offset = 0	-----
	CFP intervals (sec) = 0.01	-----
	Max failed polls = 2	-----
	Beacon interval (secs) = 1	-----
Wlan_PCF1	Wireless LAN Parameters	
	AP.functionality=enabled	Data rate = 11Mbps
	Data rate = 11Mbps	-----
	PCF parameters	
	PCF functionality = enabled	-----
	CFP Beacon multiple =1	-----
	CFP Offset = 0	-----
	CFP intervals (sec) = 1E-250	-----
	Max failed polls = 2	-----
	Beacon interval (secs) = 1	-----

Tabla 15. Configuración de los atributos en los equipos de *Wlan_access_point_PCF* y *Wlan_PCF*.

Corremos la simulación por un tiempo de 120 segundos, recolectamos las estadísticas globales de la WLAN y obtenemos los siguientes resultados:

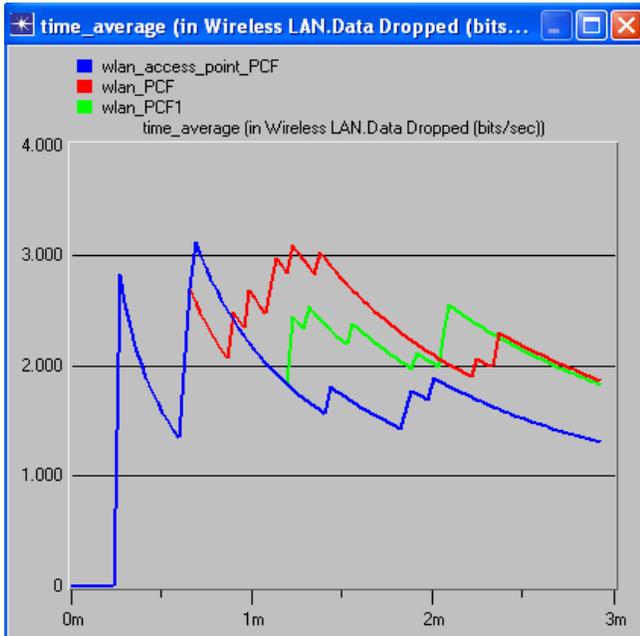


Fig 81. Comparación Data dropped de la WLAN.

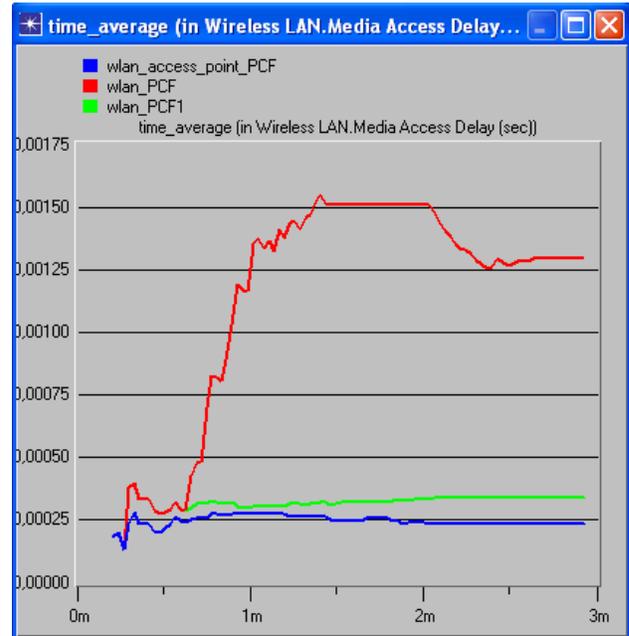


Fig 82. Comparación media access delay WLAN.

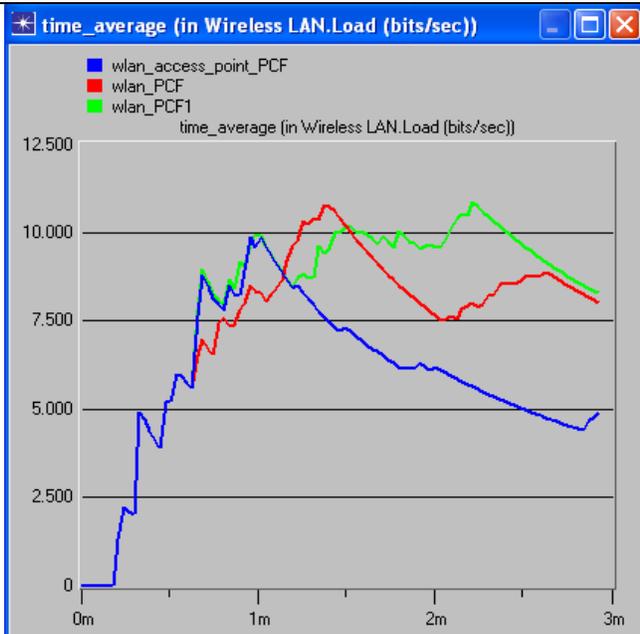


Fig 83. Comparación Load de la WLAN.

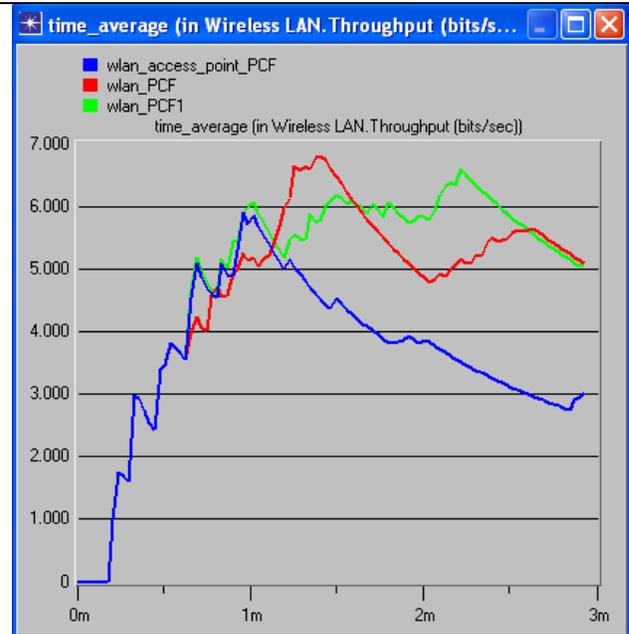


Fig 84. Comparación Throughput WLAN.

5.6.1 Análisis de resultados.

En el modo PCF las estaciones acceden al medio inalámbrico coordinadas por un Punto de Coordinación (Point Coordinator: PC) que encuesta a los nodos si desean o no transmitir. El modo PCF tiene prioridad más alta que DCF, ya que puede comenzar a transmitir después de un tiempo más corto que DIFS; este tiempo es llamado Espacio Inter-Tramas de la Función de Coordinación Puntual (PCF Inter-Frame Space: PIFS). El tiempo se divide en periodos repetidos llamados supertramas (superframes), donde se alternan Periodos Libres de Contención (Contention Free Period: CFP) y Periodos de Contención (Contention Period: CP). Un CFP seguido de un CP es una super-trama. Durante el CFP, se usa la PCF para acceder el medio mientras que durante el CP se usa la DCF. Un super-frame comienza con un frame de alerta: beacon), independientemente si la PCF está o no activa.

El “beacon” es un paquete de administración que sirve para sincronizar los relojes locales en las estaciones. Para que las estaciones accedan al medio compartido, el PC genera mensajes de “beacon” a intervalos regulares, las cuales informan a las estaciones bases que un nuevo CFP ha comenzado. El PC pregunta a una estación si desea transmitir. En caso de no obtener respuesta después de un PIFS, pregunta a otra estación o da por terminado el CFP. A partir de lo anterior es claro que durante un CFP el canal no permanece desocupado por un periodo mayor a PIFS.

De acuerdo a las graficas se puede comprobar que efectivamente el proceso descrito anteriormente debe estar sucediendo, ya que si observamos la figura 82 de acceso al medio, podemos observar como aumenta o disminuye este parámetro al modificar el intervalo CFP, lo que quiere decir que los nodos toman mas o menos tiempo en acceder al medio de acuerdo al valor asignado al intervalo CFP. Lo cual es totalmente correcto ya que durante el intervalo CFP, el punto de

coordinación se encarga de asignar el orden de acceso al medio de cada una de las estaciones.

Con respecto a los paquetes enviados y recibidos (Fig. 83 y 84) observamos como al modificar los parámetros PCF, estos parámetros aumentan, lo que quiere decir que hubo una mejora con el mecanismo activado.

Lo único es que hubo pérdida de datos significativo para todos los escenarios (Fig. 81), lo que significa que a pesar de la mejora que hubo en los distintos parámetros de la red, la pérdida de datos se mantiene siempre constante.

De este escenario podemos finalmente concluir que este parámetro es un parámetro realizado para modificar la forma como trabaja un punto de acceso, por decirlo de algún modo: este es un parámetro que permite ***sintonizar el funcionamiento de un punto de acceso.***

6 CONCLUSIONES

Los productos de redes inalámbricos no han sido muy bien recomendados durante algún tiempo. Solo recientemente estas tecnologías se han desarrollado hasta el punto que hoy en día son consideradas herramientas profesionales. La tecnología inalámbrica que esta mas cerca de emular el comportamiento de las redes de los equipos de cables son las redes WLAN que fueron el objetivo principal de este documento. No son exactamente lo mismo que una red cableada, pero es más que suficiente para el desarrollo de algunas tareas de red.

Durante este documento tratamos los diferentes escenarios sobre los que actúa una red inalámbrica. Se comprobaron cada uno de los conceptos y en base a esto se obtuvieron conclusiones.

Para trabajar con una red inalámbrica de manera óptima es necesario entender perfectamente todos y cada uno de los conceptos de sistemas inalámbricos, ya que si no se tienen estos conocimientos se terminara instalando una red pobre, poco fiable de pobre rendimiento. Recuerde los resultados obtenidos y analice el rendimiento que necesita para su red: si necesita un máximo rendimiento para su red y no le importa mucho la movilidad, entonces una red cableada es mejor para usted. Pero si a usted le gusta estar con la tecnología de punta, no le gusta cablear su casa u oficina, analice el rendimiento que necesita para su red y entre en la tecnología del nuevo milenio.

7 GLOSARIO

Access control: (control de acceso) Es la forma de evitar el uso no autorizado de los recursos de la red.

Access point (AP): (punto de acceso) Una estación que ofrece los DSS a sus estaciones asociadas.

Basic service area (BSA): (área de servicio básico) región dentro de la cual los miembros de un mismo BSS se pueden comunicar.

Basic service set (BSS): (conjunto de servicios básicos) Un grupo de estaciones controladas por una misma función de distribución.

Beacon frame: Los AP mandan estas tramas periódicamente a broadcast, informando sobre las capacidades de la BSS que forman, sus propiedades y demás información de interés para las STAs.

Broadcast address: (dirección de difusión) Una dirección a nivel MAC que pretende direccionar a todas las STAs de la red.

Channel: (canal) Una instancia concreta del uso del medio en un área determinada que no puede ser utilizada simultáneamente por mas de una STA, debido a la interferencia. Algunos modelos de capas físicas ofrecen un solo canal, mientras que otros, permiten el uso de varios canales.

Coordination function: (función de coordinación) La manera que tiene una STA, operando en un BSS de saber si puede transmitir y recibir tramas MAC por el WM.

Distributed coordination function (DCF): (función de coordinación distribuida)
Es un tipo de función de coordinación que esta activa en todos los STA's de la BSS.

Distribution system (DS): (sistema de distribución) Los sistemas usados para interconectar diferentes BSS, y otras LANs entre si.

Distribution system services (DSS): (servicios del sistema de distribución) Servicios a nivel MAC que permiten a STAs de diferentes BSSs o estaciones de otras redes 802, comunicarse entre si. Los AP ofrecen estos servicios a sus BSS y han de estar conectados a un DS.

Extended service set (ESS): (conjunto de servicio extendido) Cuando varias BSS están interconectadas mediante un DS, forman entre si un ESS.

Independent service set (IBSS): (conjunto de servicio independiente) La BSS formada por las STAs de una red ad-hoc.

Mobile station: (estación móvil) STA que accede a la red mientras esta en movimiento.

Multicast address: (dirección de multidifusion) Dirección a nivel MAC que engloba a un grupo de STAs.

Network allocation vector (NAV): (vector de asignación de red) Es un indicador, localizado en cada STA, de los periodos de tiempo en los que una STA no puede iniciar una transmisión, independientemente de si el WM este libre para transmitir.

Point coordination function (PCF): (función de coordinación centralizada) Un tipo de función de coordinación que esta activa en un único STA de la BSS.

Portable station: (estacion portatil) Una STA que aunque puede cambiar de localización, solo transmite/recibe cuando esta quieta.

Station (STA): (estación) Cualquier dispositivo que contiene un interfaz 802.11.

Wireless medium (WM): Medio de transmisión sin cables, en concreto el aire.

8 ABREVIATURAS Y ACRONIMOS

ACK acknowledgment (asentimiento)

AP Access Point (punto de acceso)

BSA Basic Service Area (área de servicio básico)

BSS Basic Service Set (conjunto de servicio básico)

CSMA Carrier Sense Multiple Access (acceso múltiple por detección de portadora)

CSMA/CA CSMA with Collision Avoidance (CSMA con política de prevención de colisiones)

CSMA/CD CSMA with Collision Detection (CSMA con política de detección de colisiones)

CTS Clear To Send (permiso para enviar)

DCF Distribution Coordination Function (funcion de coordinacion distribuida)

DIFS Distributed Inter Frame Space (tiempo entre tramas para estaciones)

DS Distribution Service (servicio de distribución)

IEEE Institute of Electrical and Electronics Engineers

MAC Medium Access Control (control de acceso al medio)

Mbps Mega bits por segundo

NAV Network Allocation Vector (vector de reserva del medio)

PCF Point Coordination Function (funcion de coordinacion centralizada)

OSI Open Systems Interconnection

PIFS Point Inter Frame Space (tiempo entre tramas para el AP)

RTS Request To Send (solicitud para enviar)

SIFS Short Inter Frame Space (tiempo entre tramas para ACK)

VCS Virtual Carrier Sense (detección portadora virtual)

9 BIBLIOGRAFIA.

- [1] LAN MAN Standards Committee of the IEEE Computer Society, "Part 11: wireless LAN medium access control (MAC) and physical layer (PHY) specifications," ANSI/ IEEE Standard 802.11, 1999 Edition.
- [2] OPNET Technologies, Inc., "Wireless LAN model description," http://www.opnet.com/products/library/WLAN_Model_Guide1.pdf.
- [3] http://en.wikipedia.org/wiki/Main_Page.
- [4] Craig Zacker. Redes Manual de referencia. McGraw-hill Osborne Media.
- [5] S. Xu and T. Sadawi, "Revealing the Problems with 802.11 MAC Protocol in Multihop Wireless Networks", Computer Networks, Volume 38, N. 4, March 2002
- [6] Gonzalo López. Modulo Redes de computadores con OPNET IT. Minor en telecomunicaciones 2005 – 2006.
- [7] Alberto Cortes Marín. Entendiendo las redes 802.11a Versión 0.9. 8 de Enero del 2004.