PFC

Redes inalámbricas y simulación de WLAN mediante OPNET

Walter Rafael Romero Kanashiro.
Dirigido por Dra. Eva Vallada Regalado.

Semestre 2012/2013-1

Índice.

0. Introducción

En los últimos años las redes inalámbricas se han convertido en una de las tecnologías más prometedoras. Las WLAN están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Pero no solamente nos las encontramos en entornos locales, sino que también se extienden a ambientes públicos, en áreas metropolitanas, como medio de acceso a internet para cubrir zonas de alta densidad de usuarios.

Entre sus ventajas encontramos:

- No existen cables físicos
- Suelen ser más baratas
- Permiten gran movilidad dentro del alcance de la red
- Suelen instalarse fácilmente

Aunque también cabe tener en cuenta ciertos inconvenientes:

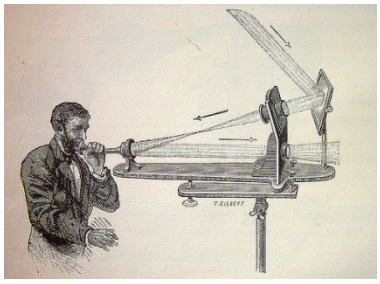
- Todavía no hay estudios certeros sobre la peligrosidad (o no) de las radiaciones utilizadas en las comunicaciones inalámbricas
- Pueden llegar a ser más inseguras, ya que cualquier host cercano podría acceder a la red. De todas formas los aspectos de seguridad de las conexiones inalámbricas han ido mejorando rápida y eficazmente.

A pesar de los inconvenientes, las ventajas priman sobre estos y las redes inalámbricas se han convertido en la solución más barata y práctica para usuarios domésticos y empresas, haciendo posible mantener una conexión incluso en los lugares donde el cable no ha llegado.

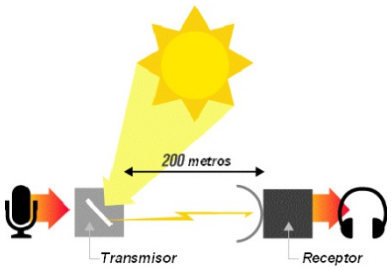
1. Historia de las redes inalámbricas

Para empezar a hablar de redes inalámbricas es necesario que nos remontemos al año 1880, en el que Graham Bell y Summer Tainter inventaron el primer aparato de comunicación sin cables, el fotófono pero no tuvo mucho éxito debido a que entonces todavía no se distribuía electricidad y las primeras bombillas se habían inventado un año antes.

El Fotófono fue un dispositivo que permitía la transmisión de sonido por medio de una emisión de luz. El dispositivo utilizaba celdas sensibles a la luz elaboradas con cristal de selenio, una de sus propiedades es que la resistencia eléctrica varía inversamente con la iluminación. El principio básico consistía en modular una emisión de luz directamente al receptor, fabricado en selenio, que era donde se conectaba el teléfono. La modulación era hecha por un espejo vibratorio o por un disco que periódicamente obscurecía el haz de luz.



En un experimento en Washington, el emisor y el receptor fueron situados en diferentes edificios a unos 200 metros de separación. El emisor consistía en un espejo que dirigía la luz del sol para ser modulado por un espejo vibratorio y enfocado por un lente que lo dirigía al receptor, el receptor consistía de un reflector parabólico con las celdas de selenio en el foco y un teléfono incorporado.



Fue patentado el 18 de diciembre de 1880, aunque la calidad de comunicación permaneció pobre y la investigación no fue continuada por Bell. Este invento sirvió como base al desarrollo de las comunicaciones usando fibra óptica y láser.

En 1888 el físico alemán Rudolf Hertz realizó la primera transmisión si cables con ondas electromagnéticas mediante un oscilador que uso como emisor y un resonador que hacía de receptor. En 1894 las ondas de radio ya eran un medio de comunicación. En 1899 Guillermo Marconi consiguió establecer comunicaciones inalámbricas a través del canal de La Mancha.

Alejandro Marconi. Fue el creador de la radiotelegrafía, o telegrafía sin hilos. En 1895 realizó la primera transmisión sin hilos a 1 km de distancia. En 1899 consiguió hacer el primer enlace a través del canal de La Mancha (48 Kms).

En 1907 se transmitían los primeros mensajes completos a través del Atlántico. Durante la Segunda Guerra Mundial se produjeron importantes avances en este campo.

La primera red inalámbrica no tuvo lugar hasta 1971, cuando un grupo de investigadores, en la universidad de Hawái, dirigidos por Norman Abramson crearon el primer sistema de conmutación de paquetes mediante una red de comunicación por radio, dicha red se llamó ALOHA.

> **ALOHAnet** (o simplemente ALOHA) fue un sistema de redes de ordenadores desarrollado en la universidad de Hawái. Estaba formada por 7 ordenadores situadas en distintas islas que podían comunicar con un ordenador central al cual pedían que realizara cálculos. ALOHAnet era una autentica red, todos los ordenadores podían enviar datos en cualquier momento sin necesidad de intervención por parte de un operador, y podía haber cualquier numero de ordenadores, al ser una transmisión por radio, no había costes fijos, por lo que el canal se dejaba abierto y se podía usar en cualquier momento. Se presentaba la problemática producida si dos sistemas en la red enviaban al mismo tiempo, ambas señales se estropearían. Para solventarlo se usó una nueva solución, que mas tarde se convertiría en el estándar, el Acceso múltiple por detección de portadora (CSMA). Un año después ALOHA se conecto mediante ARPANET al continente americano.

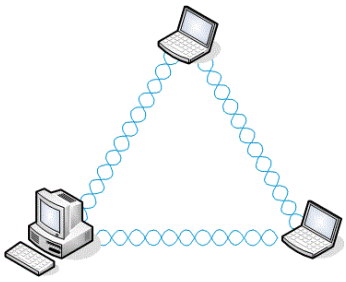
A finales de los sesenta se publicaron los resultados de un experimento consistente en utilizar enlaces de infrarrojos para crear una red local en una fábrica llevado a cabo por IBM en Suiza.

Como hemos visto se usan ondas electromagnéticas para transportar información de un punto a otro, para este objetivo se hace uso de ondas portadoras (la señal que contiene la información a transmitir). La onda moduladora se acopla con la portadora, a esto se le llama modulación, surgiendo una señal de radio que ocupa más de una frecuencia debido a que la frecuencia de la primera se acopla a la segunda. Gracias a esto pueden existir varias portadoras simultáneamente en el mismo espacio sin interferirse, siempre y cuando se transmitan en diferentes frecuencias. Otra ventaja es la mayor facilidad en la transmisión de la información. Resulta más barato transmitir una señal de alta frecuencia (como es la modulada) y el enlace es mayor. El receptor se sintoniza para seleccionar una frecuencia de radio y rechaza las demás, tras esto demodula la señal para obtener los datos originales. A grosso modo este es el funcionamiento de las redes inalámbricas.

Para que las redes inalámbricas se pudieran expandir sin problemas de compatibilidad había que establecer unos estándares, por ello IEEE creó un grupo de trabajo especifico llamado 802.11, se definiría con este estándar el uso del nivel físico y de enlace de datos de red, especificando sus normas de funcionamiento. La diferencia entre una red inalámbrica y otra que no lo es reside en la forma en que se transmiten los paquetes de datos, el resto es idéntico y como consecuencia todo el software que vaya a funcionar con la red no debería tener en cuenta que tipo de red es ya que ambos tipos de redes son totalmente compatibles.

IEEE 802.11 define dos modos básicos de operación:

- Ad-hoc: los terminales se comunican libremente entre sí, se suele encontrar en entornos militares, operaciones de emergencias, redes de sensores, comunicación entre vehículos, etc.



- Infraestructura: los equipos están conectados con uno o más puntos de acceso al medio, es mayoritario, podemos ver este modo de operación en hogares, empresas e instituciones públicas

En 1999 Nokia y Simbol Technologies crearon la asociación Wireless Ethernet Compatatibility Alliance (WECA), que en 2003 fue renombrada a WI-FI Alliance (Wireless Fidelity) con el objetivo de crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos.

En 2000 la WECA certifico según la norma 802.11b (revisión del 802.11 original) que todos los equipos con sello Wi-Fi podrán trabajar juntos sin problemas.

802.11b utilizaba la banda de 2,4Ghz y alcanzaba una velocidad de 11Mbps. Posteriormente surgiría 802.11ª que generó problemas dado que usaba la banda de 5Ghz que, si bien esta libre en Estados Unidos, en Europa estaba reservada para fines militares.

En 2003 tras costosas deliberaciones vio la luz el 802.11g que funcionaba en la misma banda que 802.11b, pero tenía una velocidad máxima de 54Mbps.

Los tres estándares (“a”, “b” y “g”) eran incompatibles. Para resolver esta situación se comenzó a producir hardware capaz de saltar entre estas tres especificaciones sin cortar la conexión. Europa puso la banda de 5Ghz a disposición de uso civil. Actualmente hay otras tecnologías que usan estas frecuencias, como el Bluetooth.

Hoy en día el estándar vigente en el software común es el 802.11n que va en los 2,4Ghz y 5Ghz simultáneamente con una velocidad de 108Mbps.

Con el nombre de 802.11-2012 IEEE ha publicado la cuarta revisión de su estándar de comunicaciones inalámbricas 802.11 que permite ahora alcanzar velocidades de hasta 600 Mbps por canal o incluso funcionar en la banda de 3650-3700 MHz (previa solicitud de licencia). Esta nueva revisión no es la prometida versión 802.11ac, con la que se esperaba superar la barrera de 1Gbps, sino un estándar intermedio a la espera que se terminen las especificaciones oficiales de esta última.

Actualmente existe una norma de transmisión de datos llamada WIMAX (IEEE 802.16) que utiliza las ondas de radio en las frecuencias 2,5 y 5Ghz, es una tecnología dentro de las conocidas como tecnologías de última milla. Está diseñada para dar servicios de banda ancha en zonas donde el despliegue de cable o fibra por baja densidad de población representa unos costes por usuarios muy elevados. Este sistema cubre distancias de hasta 80km y una velocidad máxima de 75Mbps.

2. Tecnologías de conectividad inalámbrica

Existen dos categorías de las redes inalámbricas:

1. Larga distancia: son utilizadas para distancias grandes como puede ser otra ciudad u otro país.
2. Corta distancia: son utilizadas para un mismo edificio o en varios edificios cercanos no muy retirados.

Según su cobertura, se pueden clasificar en diferentes tipos:

1. Wireless Personal Area Network (WPAN): de cobertura personal, existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth (protocolo que sigue la especificación IEEE 802.15.1) ZigBee (basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías) RFID (sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto mediante ondas de radio).
2. Wireless Local Area Network (WLAN): podemos encontrar tecnologías inalámbricas basadas en HIPERLAN, un estándar del grupo ETSI, o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.
3. Wireless Metropolitan Area Network (WMAN): para redes de área metropolitana se encuentran tecnologías basadas en WiMax (Worldwide Interoperability for Microwave Acces), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMAX es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service).
4. Wireless Wide Area Network (WWAN): difiere de una WLAN en que usa tecnologías de red celular de comunicaciones móviles como WiMAX (aunque se aplica mejor a redes WMAN), UMTS (Universal Mobile Telecomunication System), GPRS, EDGE, CDMA2000, GSM, CDPD, Mobitex, Hspa y 3G para transmitir datos.

2.1. Wireless Personal Area Network (WPAN)

Como habíamos mencionado una red inalámbrica de área personal WPAN incluye redes inalámbricas de corto alcance que abarcan un área de algunas decenas de metros. Se usa generalmente para conectar dispositivos periféricos (Impresoras, teléfonos móviles, headsets, auriculares, etc.) a un ordenador sin conexión por cables. También se pueden conectar dos ordenadores cercanos.

La tecnología principal WPAN es Bluetooth, lanzado por Ericsson en 1994. Ofrece una velocidad máxima de 1 Mbps con un alcance máximo de treinta metros. También es conocida

como IEEE 802.15.1, tiene la ventaja de tener un bajo consumo de energía, algo que resulta ideal para usarla en periféricos de pequeño tamaño.

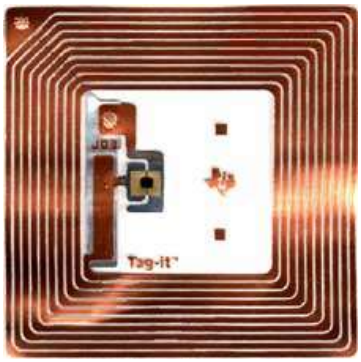
HomeRF (Home Radio Frequency), lanzada en 1998 por HomeRF Working Group (que incluye entre otros a fabricantes como Compaq, HP, Intel, Siemens, Motorola y Microsoft) ofrece una velocidad máxima de 10Mbps con un alcance de 50 a 100 metros sin amplificador. A pesar del respaldo de Intel, el estándar HomeRF se abandono en enero de 2003, principalmente porque los fabricantes de procesadores empezaron a usar tecnología Wi-Fi en placa (por medio de la tecnología Centrino, que incluía un microprocesador y un adaptador Wi-Fi en un solo componente)

La tecnología ZigBee (también conocida como IEEE 802.15.4) también se puede utilizar para conectar dispositivos en forma inalámbrica a bajo coste y con bajo consumo de energía. Resulta particularmente adecuada porque se integra directamente en pequeños aparatos (como por ejemplo electrodomésticos, sistemas de sonido y juguetes). ZigBee funciona en la banda de frecuencias 2,4GHz y en 16 canales, y puede alcanzar una velocidad de transferencia de hasta 250 Kbps con un alcance máximo de 100 metros.

Las conexiones infrarrojas se pueden utilizar para crear conexiones inalámbricas en un radio de unos pocos metros, con velocidades que pueden utilizar para crear conexiones inalámbricas de unos pocos metros, con velocidades que pueden alcanzar unos pocos megabits por segundo. Esta tecnología se usa ampliamente en aparatos electrónicos del hogar (como controles remotos). Pero puede sufrir interferencias debidas a las ondas de luz.

Infrared Data Association (IrDA) define un estándar físico en la forma de transmisión y recepción de datos por rayos infrarrojo. Se crea en 1993 entre HP, IBM, Sharp y otros. Esta tecnología está basada en rayos luminosos que se mueven en el espectro infrarrojo. Los estándares IrDA soportan una amplia gama de dispositivos eléctricos, informáticos y de comunicaciones, permite comunicación bidireccional entre dos extremos a velocidades que oscilan entre los 9600bps y los 4Mbps. Esta tecnología se encontraba en muchos ordenadores portátiles y teléfonos móviles de finales de los noventa. Fue gradualmente desplazada por tecnologías como Wi-Fi y Bluetooth.

RFID (Radio Frequency Identification) es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivo denominados como etiquetas, tarjetas, transpondedores o tags RFID. El propósito fundamental es transmitir la identidad de un objeto mediante ondas de radio. Las etiquetas RFID son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas si la requieren, no se requiere visión directa entre emisor y receptor.



2.2 Wireless Local Area Network (WLAN)

WLAN es un sistema de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensiones de esta. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas. Las WLAN van adquiriendo importancia en muchos campos, como almacenes o para manufactura, en los que se transmite información en tiempo real a una terminal central. También son muy populares en los hogares para compartir el acceso a internet entre computadores.

HIPERLAN es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54Mbps en la frecuencia 5GHz.HIPERLAN/1 es un estándar de ETSI (European Telecomunications Standards Institute). HIPERLAN/2 es una solución estándar para un rango de comunicación corto que permite una alta transferencia de datos y calidad de servicio del tráfico entre estaciones base WLAN y terminales de usuario. Es similar a 802.11a (5GHz). Entre las características de HIPERLAN encontramos que tiene un rango de 50 m, baja movilidad (1,4 m/s), soporta trafico asíncrono y síncrono, sonido 32 Kbps con una latencia de 10 ns, video 2Mbits/s con una latencia de 100ns y una velocidad para datos de 10Mbps La seguridad está provista por lo último en técnicas de cifrado y protocolos de autenticación.

2.2.1 El estándar IEEE 802.11

El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI, especificando sus normas de funcionamiento en un WLAN.

Principales Estándares 802.11

802.11 Legacy: la versión original del estándar IEEE 802.11 publicada en 1997 especifica dos velocidades de transmisión teóricas de 1 y 2Mbps que se transmiten por señales infrarrojas en la banda ISM 2,4GHz. IR sigue siendo parte del estándar, pero no hay implementaciones posibles. El estándar original también define el protocolo CSMA/CA (múltiple acceso por detección de portadora evitando colisiones) como método de acceso. Una parte importante de la velocidad de transmisión teórica se utiliza en las necesidades de esta codificación para mejorar la cantidad de la transmisión bajo condiciones ambientales diversas, lo cual se tradujo en dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue el primero de esta familia en alcanzar amplia aceptación entre los consumidores.

> CSMA/CA es un protocolo de control de acceso a redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos. De esta forma el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio esta libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. Se utiliza en canales en los que por naturaleza no se puede usar CSMA/CD. Para enviar una trama, el equipo origen primero envía una trama corta de control de solicitud de transmisión RTS (Request To Send). Este mensaje de control contiene las direcciones MAC del equipo origen y destino. Si el equipo destino recibe esta trama significa que está preparado para recibir una trama. Este equipo devolverá una trama de contestación: preparado para transmitir CTS (Clear To Send) o receptor ocupado (RxBUSY). Si la respuesta es afirmativa el equipo origen transmite la trama en espera (DATA). Si el equipo de destino recibe correctamente el mensaje contesta con la trama de confirmación positiva ACK (ACKnowledged) y si no la recibe correctamente contesta con la trama de contestación negativa NAK (NAKnowledged) y el equipo origen tratara de volver a enviarlo. Este procedimiento se repite un número predefinido de veces hasta conseguirse una transmisión correcta de la trama DATA.

802.11a: la revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos base que el estándar original, opera en la banda de 5GHz y utiliza 52 subportadores ortogonal frecuency-division multiplexing (OFMD) con una velocidad máxima de 54Mbps, lo que lo hace un estándar practico para redes inalámbricas con velocidades reales de aproximadamente 20Mbps. La velocidad de datos se reduce a 48, 32, 24, 12, 9 o 6Mbps en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos de estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Dado que la banda de 2,4 GHz tiene gran uso, el utilizar la banda de 5GHz representa una ventaja del estándar 802.11a, dado que se presentan menos interferencias. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos 802.11a únicamente puntos en línea de vista, con lo que se hace necesaria la instalación de un mayor número de puntos de acceso. Esto significa también que los equipos que trabajan con este estándar no pueden penetrar tan lejos como los del estándar 802.11b, dado que sus ondas son más fácilmente absorbidas.

> La multiplexación por división de frecuencias ortogonales (OFDM), es una multiplexación que consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o en PSK. Reduce la diafonía durante la transmisión de la señal.

802.11b: La revisión del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11Mbps y utiliza el mismo método de acceso CSMA/CA, en la práctica la velocidad máxima de transmisión con este estándar es aproximadamente 5,9Mbps sobre TCP y 7,1Mbps sobre UDP.

Los productos de la 802.11b aparecieron en el mercado muy rápido debido a que la 802.1b es una extensión directa de la técnica de modulación DSSS definida en el estándar original. Por lo tanto los chips y productos fueron fácilmente actualizados para soportar las mejoras del 802.11b. El dramático incremento en el uso del 802.11b junto con sustanciales reducciones de precios causó una rápida aceptación del 802.11b como la tecnología WLAN definitiva. Es usualmente usada en configuraciones punto a multipunto como en el caso de los AP (Acces Point) que se comunican con una antena omnidireccional con uno o más clientes que se encuentran ubicados en un área de cobertura alrededor del AP. El rango típico de interiores es de 32 metros a 11Mbps y 90 metros a 1Mbps. Con antenas de alta ganancia externas el protocolo puede ser utilizado en arreglos fijos punto a punto de rangos superiores de 8 Km incluso en casos de 80 a 120 Km siempre que haya línea de división. Esto se hace para reemplazar el costoso equipo de líneas o el uso de equipos de comunicaciones de microondas.

Las tarjetas 802.11b pueden operar a 11Mbps pero pueden reducirse hasta 5.5, 2 o 1Mbps en el caso de que la calidad de la señal se convierta en un problema. Dado que las tasas bajas de transferencia de información usan algoritmos menos complejos y más redundantes para proteger los datos son menos susceptibles a la corrupción debido a la atenuación o interferencia de la señal. Se han hecho extensiones del protocolo 802.11b para incrementar su velocidad a 22, 33, 44Mbps pero estas no han sido ratificadas por la IEEE. Muchas compañías llaman a estas versiones mejoradas 802.11b+. Estas extensiones han sido ampliamente

obviadas por los desarrolladores del 802.11g que tiene tasas de transferencia a 54Mbps y es compatible con 802.11b

> El espectro ensanchado por secuencia directa (DSSS), es uno de los métodos de codificación de canal (previa a la modulación) en espectro ensanchado para transmisión de señales digitales sobre ondas radiofónicas que más se utilizan. Están definidos en el estándar 802.11 para redes de área local inalámbricas WLAN.

802.11g: En Junio de 2003, se ratifico un tercer estándar de modulación: 802.11g. Este utiliza la banda 2,4GHz (al igual que el estándar 802.11b) pero opera en una velocidad teórica máxima de 54Mbps, o cerca de 24,7Mbps de velocidad real de transferencia, similar al estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatible los dos estándares. Sin embargo, en redes bajo el estándar "g" la presencia de nodos bajo el estándar "b" reduce significativamente la velocidad de transmisión. El mayor rango de los dispositivos 802.11g es ligeramente mayor que en los 802.11b pero el rango en que el cliente puede alcanzar 54Mbps es mucho más corto que en el caso de 802.11b.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Muchos de los productos de banda dual 802.11g sufren de la misma interferencia de 802.11b en el rango ya saturado de 2,4Ghz por dispositivos como microondas, dispositivos bluetooth y teléfonos inalámbricos.

802.11n: En enero de 2004, la IEEE anuncio la formación de un grupo de trabajo 802.11 para desarrollar una nueva versión del estar 802.11. La velocidad real de transmisión podría llegar a los 500Mbps (lo que significa que las velocidades teóricas de transmisión serian aun peores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b. También se espera que el alcance de operaciones de las redes sea mayor con este nuevo estándar. Existen también otras propuestas alternativas que podrán ser consideras y se espera que el estándar que debía ser completado hacia finales de 2006, se implante hacia 2008, puesto que hasta principios de 2007 no se acaba el segundo boceto. No obstante hay dispositivos que se adelantaron al protocolo y ofrecieron de forma no oficial este estándar.

802.11n se construyó basándose en las versiones previas del estándar 802.11 añadiendo MIMO (Multiple-Input Multiple-Output). MIMO utiliza múltiples transmisiones y antenas receptoras permitiendo incrementar el tráfico de datos.

2.3 Wireless Local Area Network (WLAN)

WiMAX (Worldwide Interoperability for Microwave Acces, interoperabilidad mundial para acceso por microondas) es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias 2,3 a 3,5GHz. Esta tecnología se encuentra dentro de las tecnologías llamadas de última milla, también conocidas como bucle local que permite la recepción de

datos por microondas y retransmisión por ondas de radio. El estándar que define esta tecnología es el IEEE 802.16. Una de sus ventajas es dar servicio da banda ancha en zonas donde el despliegue de cable o fibra por la baja densidad de población presenta unos costos por usuario muy elevados. El único organismo habilitado para certificar el cumplimiento del estándar y la interoperabilidad entre equipamiento de distintos fabricantes es el Wimax Forum.

Existen dos variantes:

- De acceso fijo (802.16.d), en el que se establece un enlace radio entre la estación base y un equipo de usuario situado en el domicilio del usuario. Para el entorno fijo, las velocidades teóricas máximas que se pueden obtener son de 70Mbos con un ancho de banda de 20MHz. Sin embargo, en entornos reales se han conseguido velocidades de 20 Mbps con radios de célula de hasta 6Km, ancho de banda que es compartido por todos los usuarios de la célula.
- De movilidad completa (802.16e) que permite el desplazamiento del usuario de un modo similar al que se puede dar en GSM/UMTS, el móvil, aun no se encuentra desarrollado y actualmente compite con las tecnologías LTE, (basadas en femtocelulas, conectadas mediante cable), por ser la alternativa para las operadoras de telecomunicaciones que apuestan por los servicios en movilidad, este estándar, en su variante “no licenciado”, compite con el Wi-Fi IEEE 802.11n, ya que la mayoría de los portátiles y dispositivos móviles, empiezan a estar dotados de este tipo de conectividad.

LMDS (Local Multipoint Distribution Service) es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Esta concebida de manera celular, esto es, existen una serie de antenas fijas (no móviles) en cada base, que son los sectores que prestan servicio a determinados núcleos de poblacionales, lo cual resulta muy apetecible para las operadoras, puesto que se evitan los costosos cableados de fibra óptica o de pares de cobre necesarios para dar cobertura a zonas residenciales/empresariales.

Usa señales en la banda de microondas, por lo que las distancias de transmisión son cortas, a tan altas frecuencias la reflexión de las señales es considerable. Pero también en muchos países europeos se trabaja en 3,4 – 3.5Ghz.

Tiene una distancia de enlace desde los 100m hasta 35Km dependiendo de la sensibilidad de las unidades de abonado y la calidad de servicio a ofrecer, además los sistemas de comunicación LMDS en la banda de 3,2GHz tienen la ventaja de no verse afectados por la niebla, la lluvia o la nieve.

2.4 Wireless Wide Area Network (WWAN)

Las tecnologías WWAN permiten a los usuarios establecer conexiones inalámbricas a través de redes remotas públicas o privadas. Estas conexiones pueden mantenerse a través de áreas geográficas extensas, como ciudades o países, mediante el uso de antenas en varias ubicaciones o sistemas satélite que mantienen los proveedores de servicios inalámbricos.

Tecnologías más usadas:

CDPD (Cellular Digital Packet Data): es una tecnología de transmisión de datos en terminales TDMA. Está basado en la tecnología IBM CelluPlan II, pero desarrollada por Ericsson y descontinuada a finales de los 90, que pretendía mejorar las prestaciones de la existente tecnología móvil analógica. Actualmente está apagada

GSM (Sistema Global Para las comunicaciones móviles): es un sistema estándar de telefonía móvil digital. Un cliente GSM puede conectarse a través de su teléfono móvil con su ordenador y enviar y recibir mensajes por correo electrónico, faxes, navegar por internet, acceder con seguridad a la red informática de una compañía (intranet), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el servicio de mensajes cortos (SMS) o mensajes de texto. Debido a su velocidad de transmisión y otras características se considera un estándar de segunda generación (2G).

GPRS (General Packet Radio Services): es una extensión del sistema global para comunicaciones móviles (GSM) para la transmisión de datos mediante conmutación de paquetes. Permite velocidades de transferencia de 56 a 144Kbps. Una conexión GPRS está establecida por la referencia a su nombre del punto de acceso (APN). Con GPRS se pueden utilizar servicios como Wireless Application Protocol (WAP), servicio de mensajes cortos (SMS), servicios de mensajería multimedia (MMS), Internet y para los servicios de comunicación, como el correo electrónico y la world wide web (WWW). Para fijar una conexión de GPRS para un modem inalámbrico, un usuario debe especificar el APN, opcionalmente un nombre y una contraseña de usuario y muy raramente una dirección IP, todo proporcionado por el operador de la red. La transferencia de datos de GPRS se cobra por volumen de información transmitida, mientras que la comunicación de datos a través de conmutación de circuitos tradicionales se factura por minuto de tiempo de conexión, independientemente de si el usuario utiliza toda la capacidad del canal o está en un estado de inactividad. Por ese motivo, se considera más adecuada la conexión conmutada para servicios como la voz que requieren un ancho de banda más constante durante la transmisión, mientras que los servicios de paquetes como GPRS se orientan al tráfico de datos. La tecnología GPRS como bien lo indica su nombre es un servicio

orientado a radio enlace que da mejor rendimiento a la conmutación de paquetes en dichos radio enlaces.

EDGE (Enhanced Data Rates For GSM Evolution): también conocida como EGPRS. Es una tecnología de la telefonía móvil, que actúa como Puente entre las redes 2G y 3G, se considera una evolución del GPRS esta tecnología funciona con redes GSM. Aunque EDGE funciona con cualquier GSM que tenga implementado GPRS, el operador debe implementar las actualizaciones necesarias, además no todos los teléfonos móviles soportan esta tecnología. EDGE puede ser usado en cualquier transferencia de datos basada en conmutación por paquetes, como lo es la conexión a internet. Los beneficios de EDGE sobre GPRS se pueden ver en las aplicaciones que requieren una velocidad de transferencia de datos, o ancho de banda altos, como video u otros servicios multimedia, pudiendo alcanzar una velocidad de transmisión de 384Kbps en modo paquetes.

UMTS (Universal Mobile Telecomunication System): es una tecnología usada por los móviles de tercera generación (3G), sucesora de GSM, debido a que la tecnología GSM propiamente dicha no podía seguir un camino evolutivo para llegar a brindar servicios considerados de tercera generación. Inicialmente está pensada para su uso en teléfonos móviles, pero la red UMTS no está limitada a estos dispositivos, pudiendo ser utilizada por otros. Sus tres grandes características son las capacidades multimedia, una velocidad de acceso a internet elevada (2Mbps por usuario móvil), la cual también le permite transmitir audio y video en tiempo real; y una transmisión de voz con calidad equiparable a la de las redes fijas. Además, dispone de una variedad de servicios muy extensa.

CDMA2000: es una familia de estándares de telecomunicaciones móviles de tercera generación que utilizan CDMA, un esquema de acceso múltiple para redes digitales, para enviar voz, datos, y señalización entre teléfonos móviles y estaciones base. Es una marca registrada de la Telecomunicatin Industry Association (TIA) en los Estados Unidos

Mobitex: es una tecnología que fue desarrollada por Telia, que es la PTT Sueca, como un sistema de comunicaciones privado de alarma para sus ingenieros de campo, pero luego evolucionó hacia un sistema de tipo público, habiéndose convertido en una norma mundial de facto. En Suecia la explotación comercial comenzó en 1986. Utiliza una estructura de tipo celular.

En EEUU, RAM Mobile Data (RMD) opera sistemas Mobitex en 7.700 ciudades y pueblos, cubriendo el 90 % de la población comercial y 11.000 millas de autopistas interestatales, con roaming automático a lo largo de todas las áreas de servicio.

La tecnología Mobitex está instalada o se está instalando en 16 países incluyendo: Reino Unido, Francia, Suecia, Finlandia, Noruega, Bélgica, Holanda, Australia y Chile (Compañía de Telecomunicaciones Móviles de Chile que pertenece a CTC). Existe un Mobitex Operators Association (MOA) que se ocupa de revisar las especificaciones, coordinar el software y el hardware y hacer evolucionar la tecnología. Su trabajo estimula la aparición de fabricantes de terminales. Mobitex ofrece una velocidad de 8Kbps. La penetración en Europa podría ser mayor pero tiene como competencia a la norma TETRA de trunking que está siendo

estandarizada por el ETSI. En EEUU y Canadá las frecuencias utilizadas están en la banda de 900Mhz, pero la mayoría de los otros países usan la de 450MHz

HSPA (High Speed Packet Access) es la tecnología empleada en las conexiones de internet móvil. Es una mejora del estándar UMTS con el que funcionan las redes 3G. Utiliza de forma más eficiente el espectro radioeléctrico que tienen asignado las operadoras, mejorando la velocidad y latencia en la transferencia de datos. HSPA está formado por HSDPA y HSUPA, mejoras para el canal descendente y ascendente respectivamente. Está en continua evolución gracias al trabajo del consorcio des estandarización 3GPP, que periódicamente publica las llamadas Releases, especificaciones técnicas actualizadas que mejoran el estándar.

> El Proyecto Asociación de Tercera Generación o más conocido por el acrónimo inglés 3GPP 3rd Generation Partnership Project es una colaboración de grupos de asociaciones de telecomunicaciones, conocidos como Miembros Organizativos.
> El objetivo inicial del 3GPP era asentar las especificaciones de un sistema global de comunicaciones de tercera generación 3G para móviles basándose en las especificaciones del sistema evolucionado "Global System for Mobile Communications" GSM dentro del marco del proyecto internacional de telecomunicaciones móviles 2000 de la Unión Internacional de Telecomunicaciones ITU. Más tarde el objetivo se amplió incluyendo el desarrollo y mantenimiento de:
>
> - El Sistema Global de telecomunicaciones móviles GSM incluyendo las tecnologías de radio-acceso evolucionadas del GSM (cómo por ejemplo GPRS o el EDGE).
> - Un sistema de tercera generación evolucionado y más allá del sistema móvil basado en las redes de núcleo evolucionadas del 3GPP y las tecnologías de radio-acceso apoyadas por los miembros del proyecto (cómo por ejemplo la tecnología UTRAN y sus modos FDD y TDD).
> - Un Subsistema Multimedia IP (IMS) desarrollado en un acceso de forma independiente.

3G: es una tecnología móvil que permite al usuario navegar en internet a alta velocidad sin la utilización de cables. Puede ser usada a través de un módem (para ordenadores, notebooks y netbooks) o mediante teléfonos móviles.

Ofrece:

- Mayor rapidez.
- Ofrece estar conectados permanentemente a Internet a través del teléfono móvil, pocket PC, el Tablet PC o PC portátil (Laptop).
- Recibir y enviar (en ese orden de importancia) mayor cantidad de datos por segundo.
- Promete una mejor calidad y fiabilidad, una mayor velocidad de transmisión de datos y un ancho de banda superior lo que permite que podamos tener video llamadas (ya no sucesión de fotos) con un precio módico.
- Proveer conexión a sitios de redes sociales, descargar y comprar contenidos multimedia, revisar su correo electrónico o navegar por la Web en altas

velocidades desde un teléfono móvil y una puerta para la mensajería instantánea (IM)

- Sustituir a la conexión WI-FI.
- Efectuar video llamadas, descarga y compra de música en línea, streaming de contenidos multimedia y navegación Web.

Ventajas:

- Mantener a los usuarios siempre conectados con un acceso permanente a Internet
- La posibilidad de implementar soluciones inalámbricas para entregar Internet en zonas del país con poco alcance tecnológico.

3. Seguridad en Wi-Fi

Uno de los problemas a los cuales se enfrenta actualmente la tecnología Wi-Fi es la progresiva saturación del espectro radioeléctrico, debido a la masificación de usuarios, esto afecta especialmente en las conexiones de larga distancia (mayor de 100 metros). En realidad Wi-Fi está diseñado para conectar ordenadores a la red a distancias reducidas, cualquier uso de mayor alcance está expuesto a un excesivo riesgo de interferencias.

Un muy elevado porcentaje de redes son instaladas sin tener en consideración la seguridad convirtiendo así sus redes en redes abiertas (o completamente vulnerables ante el intento de acceder a ellas por terceras personas), sin proteger la información que por ellas circulan. De hecho, la configuración por defecto de muchos dispositivos Wi-Fi es muy insegura dado que a partir del identificador del dispositivo se puede conocer la clave de éste y por tanto acceder y controlar el dispositivo se puede conseguir en sólo unos segundos.

El acceso no autorizado a un dispositivo Wi-Fi es muy peligroso para el propietario por varios motivos. El más obvio es que pueden utilizar la conexión. Pero además, accediendo al Wi-Fi se puede monitorizar y registrar toda la información que se transmite a través de él (incluyendo información personal, contraseñas….). La forma de hacerlo seguro es seguir algunos consejos:

- Cambios frecuentes de la contraseña de acceso, utilizando diversos caracteres, minúsculas, mayúsculas y números.
- Se debe modificar el SSID que viene predeterminado.
- Realizar la desactivación del broadcasting SSID y DHCP.
- Configurar los dispositivos conectados con su IP (indicar específicamente qué dispositivos están autorizados para conectarse).
- Utilización de cifrado: WPA.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP, el WPA, o el WPA2 que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos. La mayoría de las formas son las siguientes:

- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire. Este tipo de cifrado no está muy recomendado debido a las grandes vulnerabilidades que presenta ya que cualquier cracker puede conseguir sacar la clave, incluso aunque esté bien configurado y la clave utilizada sea compleja.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como dígitos alfanuméricos.
- IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.

- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados. Es lo más recomendable si solo se va a usar con los mismos equipos, y si son pocos.
- Ocultación del punto de acceso: se puede ocultar el punto de acceso (Router) de manera que sea invisible a otros usuarios.
- El protocolo de seguridad llamado WPA2 (estándar 802.11i), que es una mejora relativa a WPA. En principio es el protocolo de seguridad más seguro para Wi-Fi en este momento. Sin embargo requieren hardware y software compatibles, ya que los antiguos no lo son.

Sin embargo, no existe ninguna alternativa totalmente fiable, ya que todas ellas son susceptibles de ser vulneradas.

4. OPNET

En los últimos años se ha observado la aparición de nuevos servicios que realizan un consumo de recursos muy alto, tanto a nivel de la red como de las propias máquinas. Esto puede provocar funcionamientos defectuosos debido a la baja capacidad de las redes y los propios equipos. En algunos casos la implantación de estos servicios podría influir negativamente en partes del sistema que funcionaban correctamente. La realización de un análisis previo que permita determinar el impacto que dichos servicios pueden provocar, evitará los problemas que pudieran surgir y el consecuente descontento de los usuarios de la red. Además de evitar grandes pérdidas económicas.

OPNET (Optimized Network Engineering Tools) Technologies, Inc. es un proveedor líder de soluciones para la gestión del rendimiento de aplicaciones y redes. Ofrece la mejor solución para: la gestión del rendimiento de aplicaciones, la gestión del rendimiento de la red y la red I+D. Ofrece una amplia visibilidad y control entre dominios de infraestructura, así como la recopilación de datos y análisis profundo para poder hacer un diagnóstico poderoso sobre la raíz del problema. El software OPNET ha sido probado en miles de entornos de clientes en todo el mundo incluidas empresas y gobierno, los organismos de defensa, proveedores de servicios de red y fabricantes de equipos.

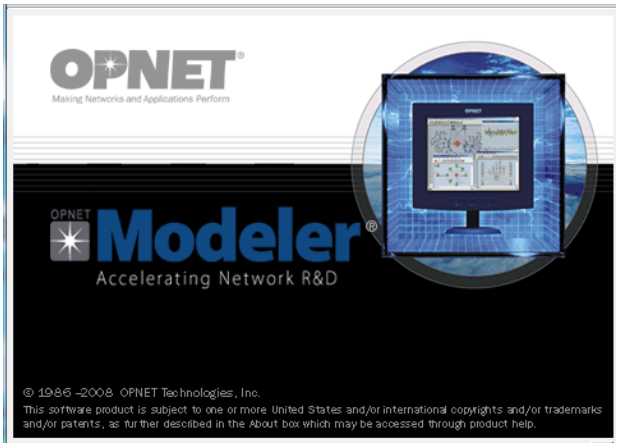
La compañía fue fundada en 1986 y comenzó a cotizar en el año 2000. Su sede reside en Bethesda, Marylan, y cuenta con oficinas en Cary, Carolina del Norte, Nashua, New Hampshire, Dallas, Texas y santa Clara, California. Cuenta con oficinas internacionales en Slough, Reino Unido, Paris, Francia; Gante, Bélgica; Frankfurt, Alemania y Singapur con el personal y los consultores en múltiples lugares en Asia y América Latina. El 29 de Octubre de 2012 fue adquirida por la tecnología Riverbed.

> Riverbed es una compañía de tecnología especializada en la mejora del rendimiento de redes y aplicaciones en red. Fue fundada el 23 de mayo de 2002 por Jerry Kennelly y McCanne Steve en San Francisco, California, donde se mantiene su sede mundial. Su producto insignia es Steelhead Appliance, un dispositivo de red que combina varias técnicas para optimizar el tráfico de datos y la utilización del ancho de banda a través de una red de área ampliada.

Entre los distintos productos que OPNET posee se encuentra OPNET Modeler para el modelado y simulación.

4.1 OPNET Modeler

Modeler es un simulador basado en eventos orientado a la simulación de redes de telecomunicaciones creado por OPNET (Optimized Network Engineering Tools).



Para ser más explícitos lo podríamos definir como un simulador dinámico y discreto que puede realizar simulaciones deterministas y/o aleatorias basándose en teorías de redes de colas.

- Dinámico porque la representación del sistema durante la simulación evoluciona con el tiempo.
- Discreto porque el comportamiento de los sistemas representados cambia únicamente en instantes de tiempo concretos, es decir, eventos.
- Una simulación es aleatoria cuando durante la simulación entran en juego variables aleatorias. En cambio, se define como determinista cuando no entra en juego ninguna variable aleatoria. En OPNET se puede definir gran cantidad de variables y asignarles un patrón determinista o aleatorio.

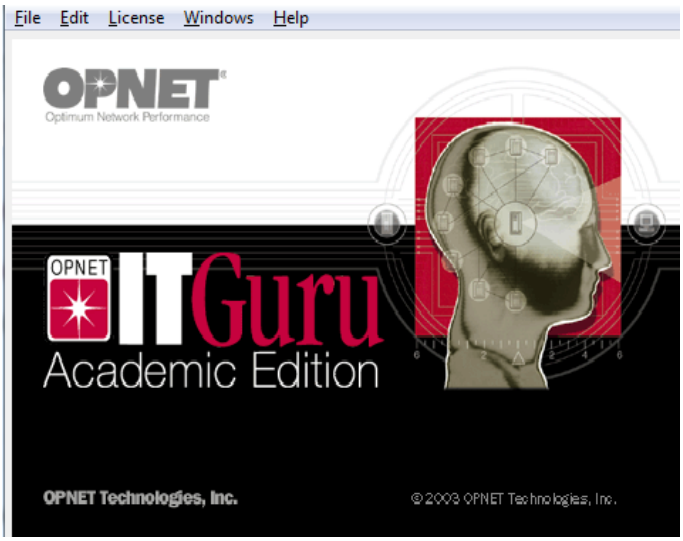
OPNET Modeler es uno de los simuladores más avanzados en el campo de las redes de telecomunicaciones. Quizás, la característica más relevante es que es un simulador orientado a objetos, lo que permite interactuar al usuario sin problemas y ofrece una gran facilidad de interpretación y creación de escenarios aparte de tener en cada objeto una serie de atributos configurables. Dispone de multitud de librerías, lo que permite simular gran diversidad de redes donde intervenga un amplio número de protocolos y variables específicas que el usuario podrá modificar y estudiar. Número de paquetes perdidos, throughput, jitter, caída de enlaces, potencia de transmisión son algunos de los parámetros que se pueden controlar. Cabe destacar que OPNET permite entre otras cosas dotar de movilidad a los nodos de la red, modificar el código fuente de las librerías de los nodos para alterar su comportamiento ante diversas acciones, definir tipos de tráfico además de carga de la red debido a tipos de servicios, como por ejemplo HTTP, correo, VoIP, streaming, etc.

5. Simulación de redes inalámbricas mediante OPNET

El proyecto consiste en la evaluación de la red inalámbrica simulada mediante OPNET. Utilizaré 2 escenarios. Un primer escenario básico para la comunicación de 2 nodos y un segundo escenario con tráfico de aplicaciones.

En el momento de implementar físicamente una red tanto de ámbito domestico como de ámbito empresarial es sumamente importante poder garantizar que esta va a funcionar de forma correcta, es decir, que todos los usuarios van a poder trabajar con la red sin que esta se llegue a saturar ni presente bloqueos. El fracaso de este diseño acarrea molestias a los usuarios, que verían afectado su nivel productividad con su repercusión en la empresa, y la corrección de este diseño genera nuevos gastos de dinero y tiempo que en un principio no estaban previstos y que con una buena planificación se hubieran podido minimizar. El objetivo general del proyecto es simular mediante OPNET el tráfico de una red antes de su implementación física para tener prácticamente asegurado el éxito de esta.

Para la realización de la simulación he utilizado el software IT Guru Academic Edition 9.1, que es el software de OPNET con fines académicos.

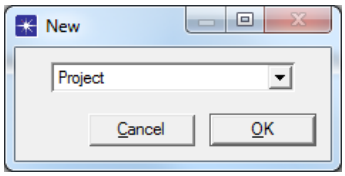


5.1 Primer escenario

En toda red, tanto inalámbrica como cableada, la conectividad es un aspecto esencial dado que sin esta no existe posibilidad de comunicación entre sus diferentes elementos. En una red de cable la conectividad física es fácil de ver, en principio valdría con ver si los equipos tienen un cable de red correctamente conectado y para su conexión lógica sería suficiente con configurar los parámetros específicos de la red. En una red inalámbrica existen los parámetros de la conexión lógica que son similares a las redes cableadas, pero las conexiones físicas no se pueden ver (a simple vista) y todas estas comparten un medio común, el aire. El objetivo parcial de este escenario es simular una conexión inalámbrica, con su respectivo tráfico, entre dos estaciones y verificar su correcto funcionamiento.

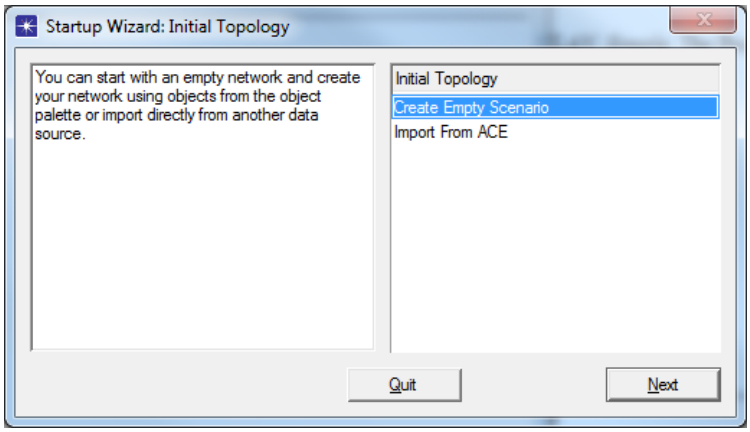
Para este primer escenario vamos a generar una red muy simple, dos estaciones, en la que se genera tráfico desde una hacia la otra, se podría hacer un escenario más simple, incluso con un solo equipo generando tráfico broadcast y monitorizando este mediante las estadísticas que nos ofrece el propio escenario, pero con dos nodos veremos cómo se hace la conexión entre estos, ya que toda conexión que se quiera hacer, por ejemplo entre un nodo y un servidor, o cualquier otro elemento de la red se hace de la misma forma. Este primer escenario, aunque básico, resulta muy útil para aprender la forma de hacer conexiones y verificar, mediante la representación de los resultados, el correcto funcionamiento de la red con el software de OPNET.

Comenzamos con la preparación del primer escenario del proyecto.

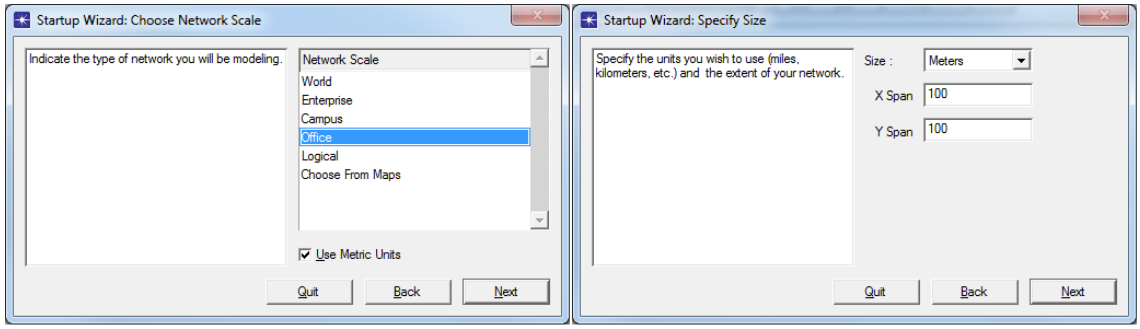


Utilizo el asistente para la creación del escenario:

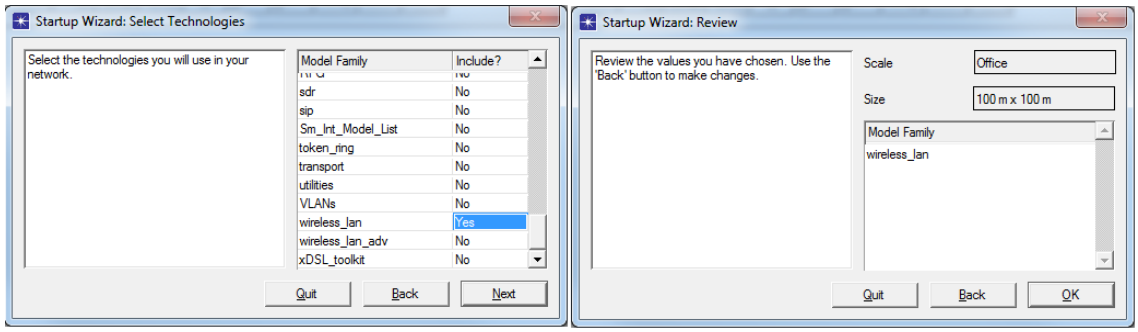
El asistente nos da las opciones de crear un escenario vacío o importarlo como topología inicial, en este caso seleccionamos crearlo vacio para empezar desde 0.



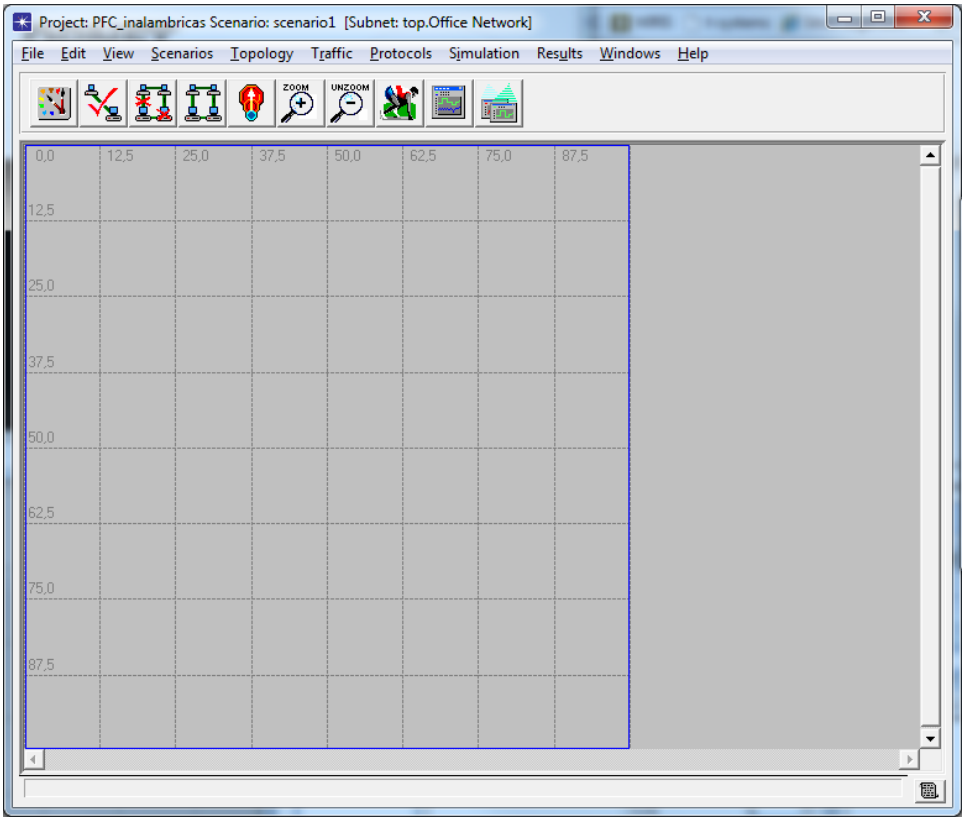
A continuación el asistente nos pide que indiquemos la escala de nuestro proyecto. OPNET nos permite trabajar desde con redes muy pequeñas, hasta redes de escala mundial. Para el proyecto seleccionamos la escala “Office” y especificamos un tamaño de oficina de 100 por 100 metros.



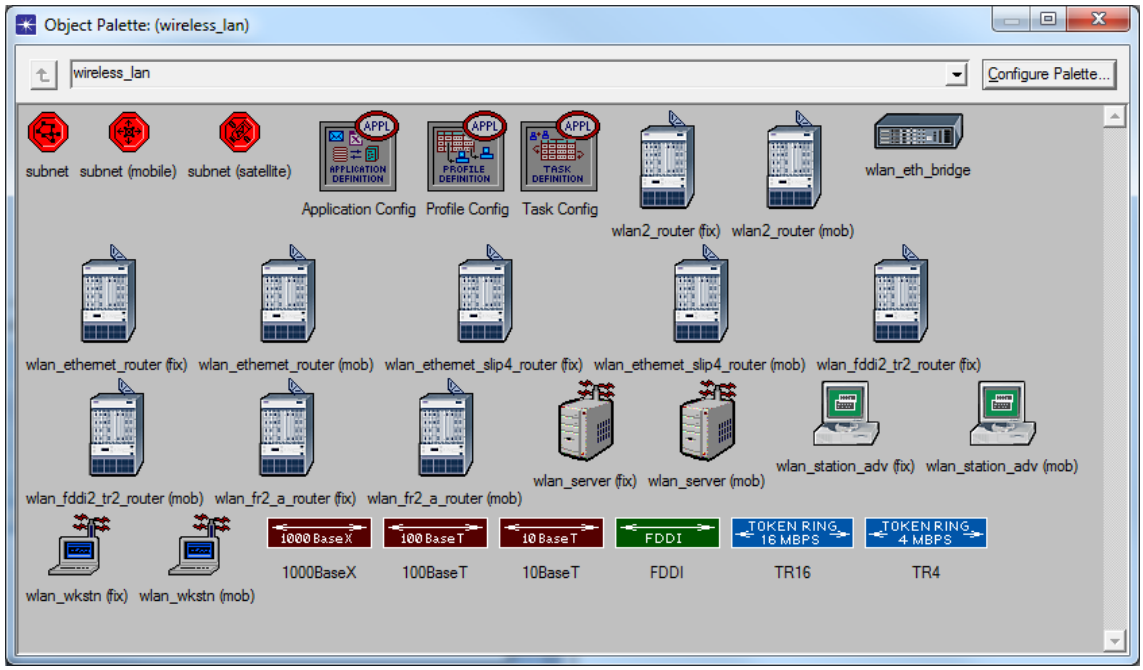
Finalmente nos permite seleccionar las tecnologías a utilizar en la red, dado que es un proyecto de redes inalámbricas seleccionamos tecnología “Wireless_lan”. Tras este paso nos muestra los valores elegidos para su revisión.



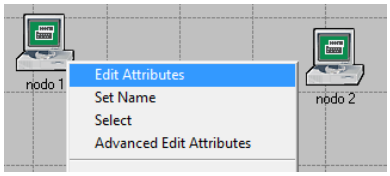
Y ya tenemos generado el escenario:



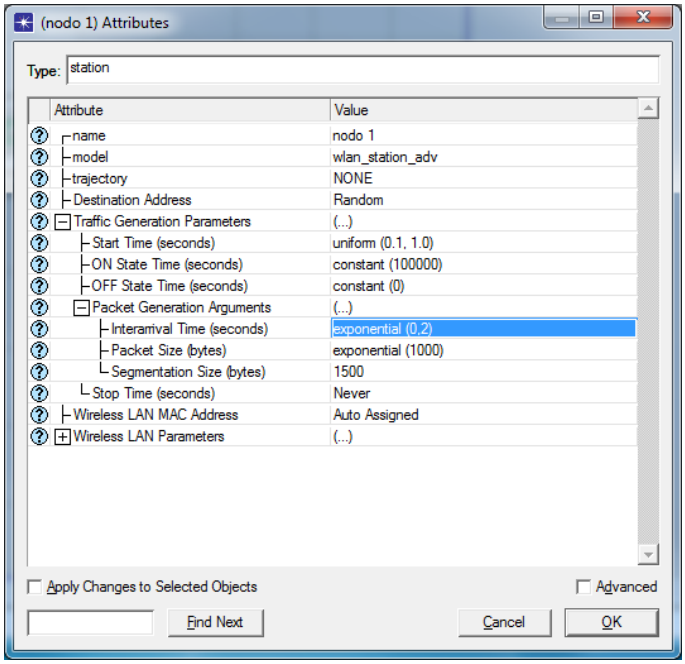
Se nos muestra también una paleta con los distintos elementos que podemos utilizar en nuestra red. En este caso elementos de tecnología inalámbrica.



Introducimos en el escenario vacío 2 wlan_station_Adv(mob)



Mediante un clic con el botón derecho sobre el nodo 1 podemos ver y editar sus atributos

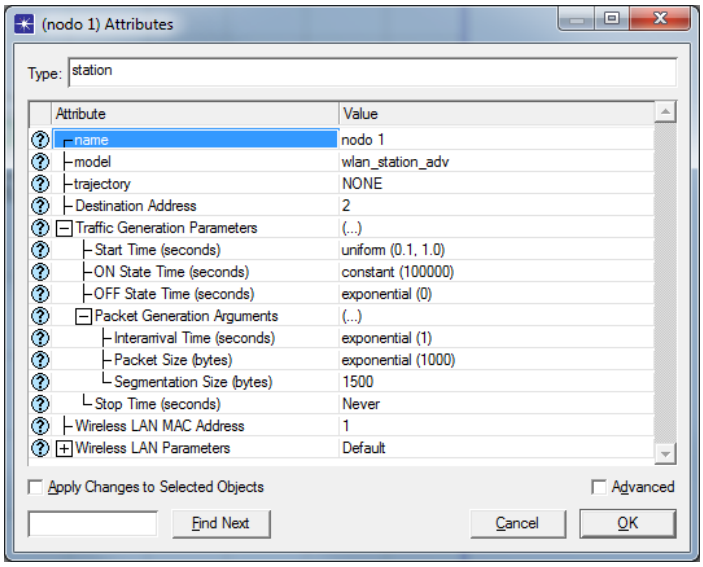


Para especificar las características del tráfico del nodo disponemos de los siguientes parámetros:

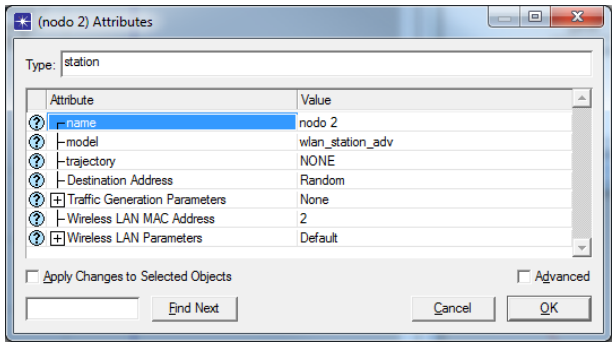
- Start Time: es el momento en que la aplicación que genera tráfico comienza. Por defecto viene con el valor "never", lo vamos a modificar dándole un valor "uniform(0.1,1.0)". Esto significa que la hora de inicio será elegida al azar de la gama 0,1 a 1,0. Es decir, en una simulación esta puede comenzar en 0,34 segundos de tiempo, pero en otra simulación podría empezar en 0,94 segundos.
- ON State Time: La aplicación genera tráfico cuando se encuentra "ON" y deja de generarlo cuando está "OFF", vamos a modificarla para que se encuentre siempre "ON" modificando el valor a "constant(10000)" segundos.
- OFF State Time: como hemos dicho, en este estado no genera tráfico. Le asignamos un valor constante 0, para que en ningún momento deje de generarlo.
- Packet Generation Arguments: cuando la aplicación se encuentra "ON" los siguientes atributos especifican el tipo de tráfico generado.
    - Interarrival Time: el tiempo entre cada paquete. La aplicación genera un paquete y espera el tiempo de llegada, acto seguido envía otro paquete, vuelve a esperar y así sucesivamente. Le asignamos un valor "exponential(1)".
    - Packet Size: el tamaño de cada paquete. Nuevamente usamos una distribución exponencial. Asignamos un tamaño de 1000 bytes al paquete.
    - Segmentation size: después de cada paquete generado, la aplicación realiza segmentación. Modificamos para que se aplique con el tamaño máximo de 1500 bytes por paquete.
- Stop Time: indica el momento en que la aplicación se detiene. Le indicamos que no se detenga nunca.

Modificaremos *Wireless LAN MAC Address* asignándole a este equipo el 1 y como dirección de destino el 2, que será asignado al otro nodo.

No realizamos más modificaciones y finalmente los atributos del nodo 1 quedan así:

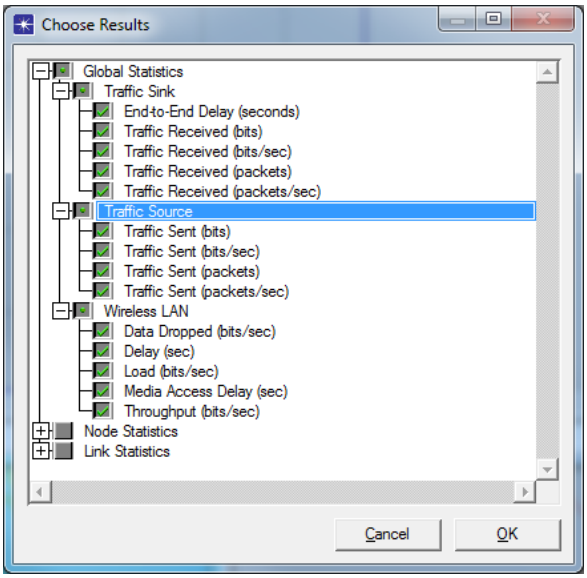


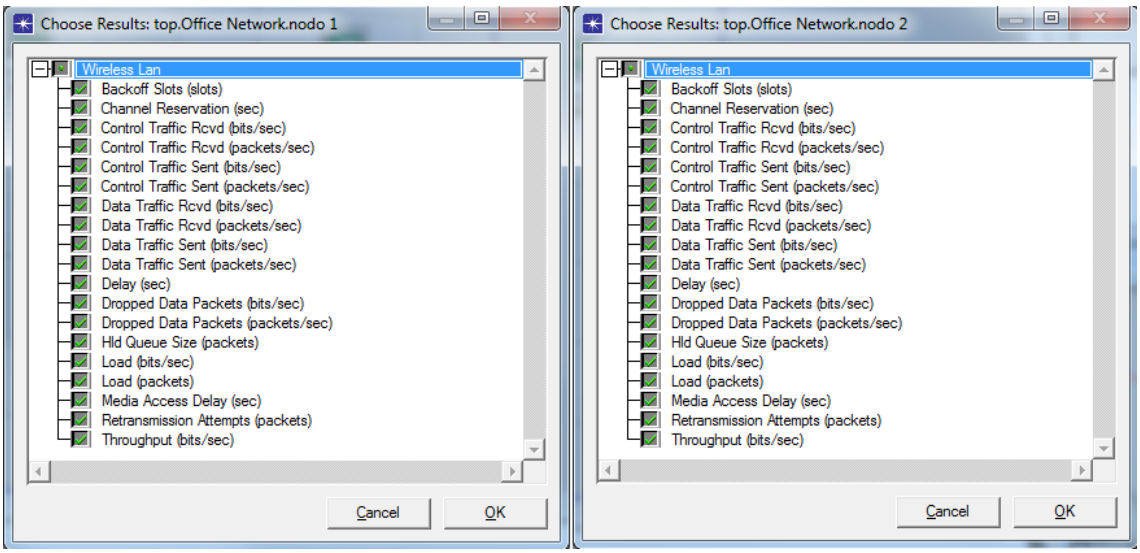
Y así el nodo 2 en el que modificamos el *Wireless LAN MAC Address* con el valor 2.



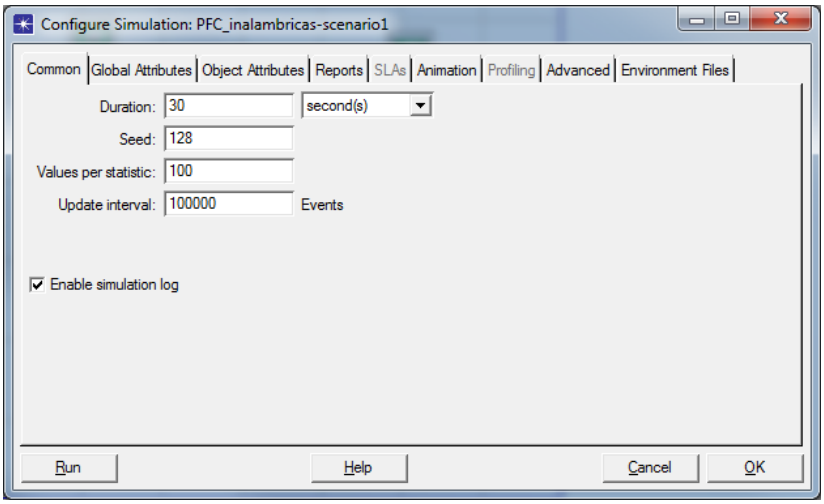
A continuación procedemos a seleccionar las estadísticas que queremos registrar, lo podemos hacer a nivel de nodo (*Choose Individual Statics*) o a nivel global.

Tanto como a nivel global como en los nodos seleccionamos todas:

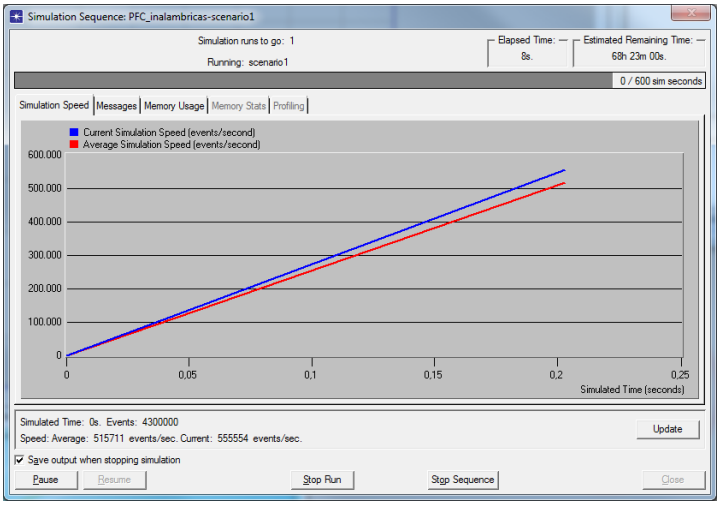




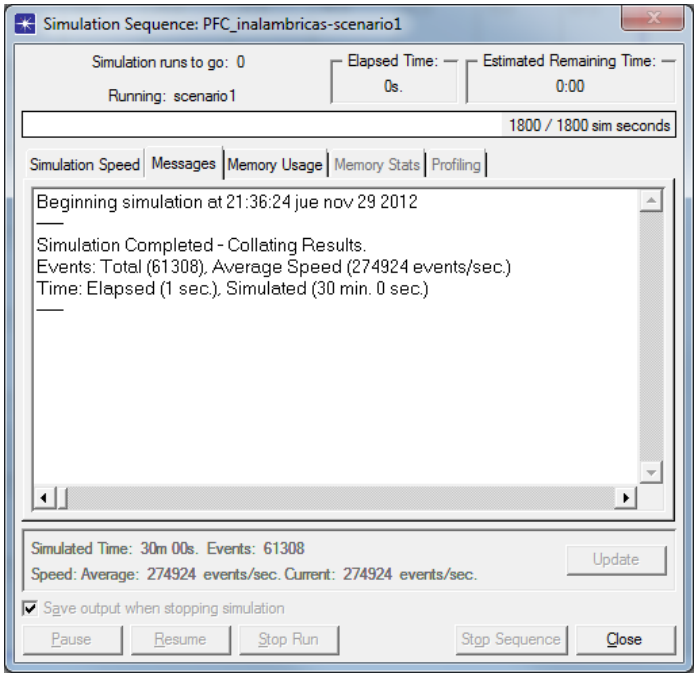
Ahora configuramos la simulación en *Simulation->Configure Discrete Event Simulation*. Modificamos para que se produzca una simulación de 30 minutos y dejamos los demás parámetros como están.



Observamos el proceso:



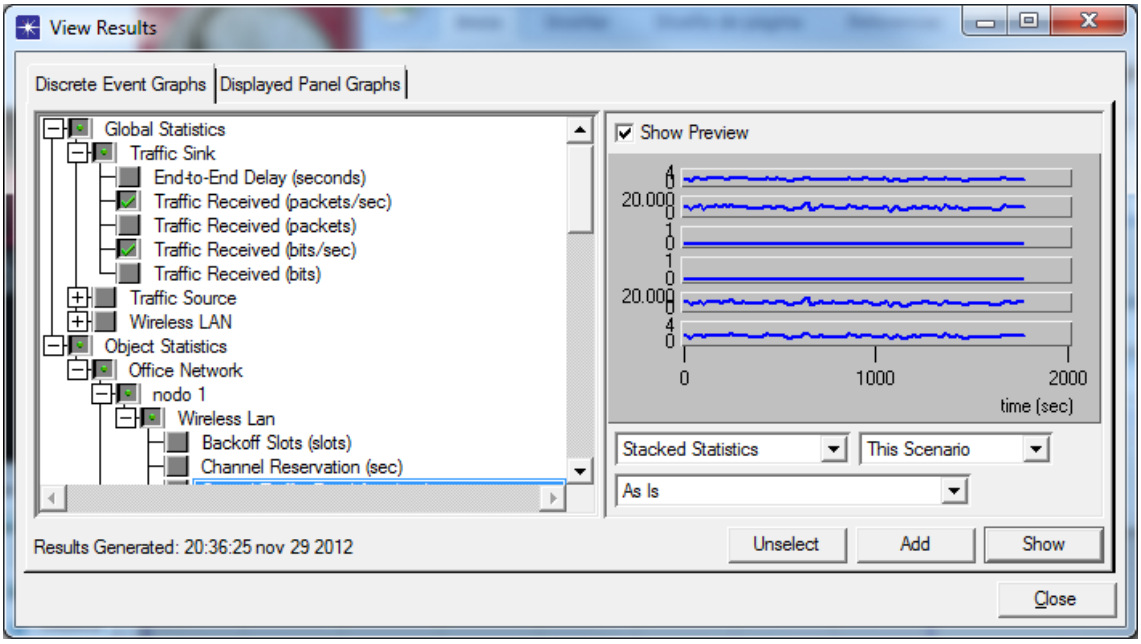
La simulación finaliza:



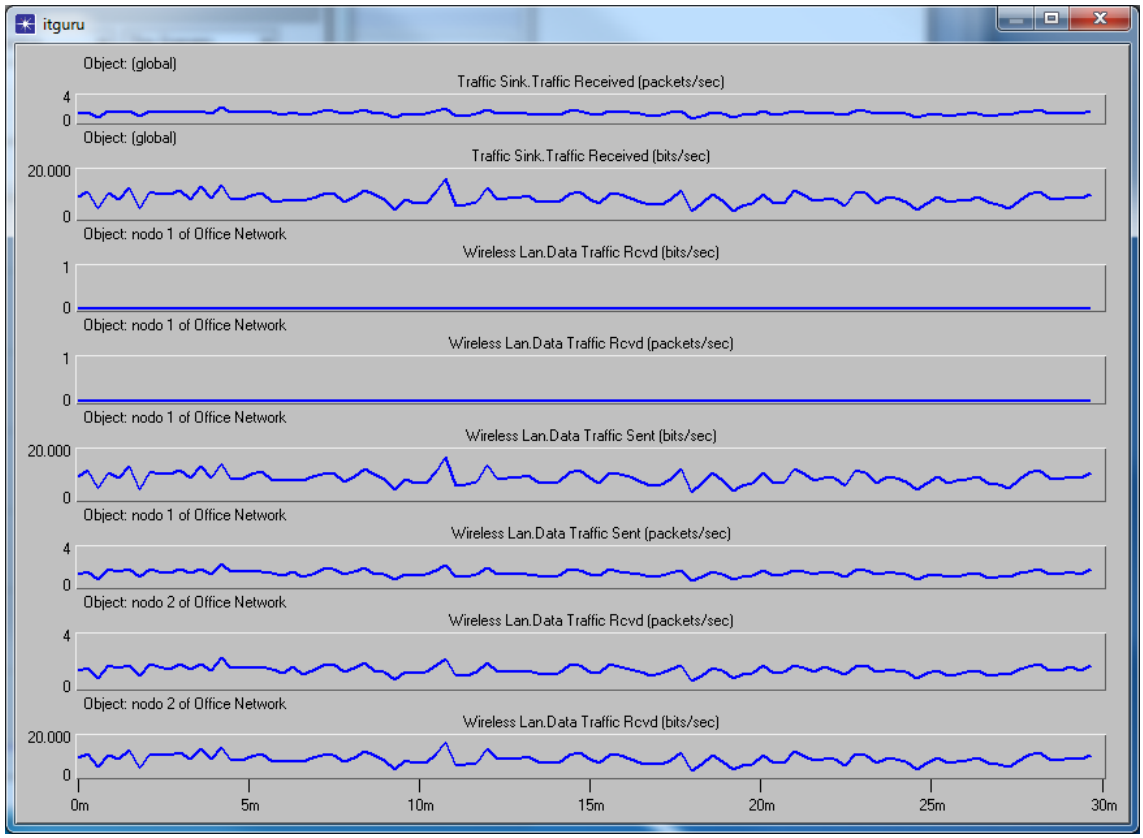
La edición académica tiene una limitación en el numero de eventos que puede simular (50 millones). Si se ejecuta una simulación y una advertencia indica que los eventos totales excedieron el límite para la edición académica se debería intentar con una simulación de duración más corta.

En este primer escenario he tenido algunos problemas al intentar una configuración en la que se generaba mucho tráfico, dado que con la elevada cantidad de eventos que generaba con un tráfico sobrecargado apenas me permitía realizar una simulación de unos pocos segundos.

Y ahora en *Results->view results* podemos seleccionar las estadísticas que queremos ver.



Según vamos seleccionando podemos ver las distintas graficas de los datos obtenidos tanto por el escenario global, y los nodos 1 y 2. A medida que estas gráficas se van seleccionando se nos va mostrado un imagen preliminar en la pantalla de la izquierda, para poder ver las gráficas al completo y en una mejor presentación. Basta con apretar el botón show una vez las que nos interesan para la evaluación están seleccionadas.



Observamos los gráficos del envío y la recepción de datos desde los puntos de vista del escenario global y de los dos nodos.

Las dos primeras graficas corresponden al escenario global, podemos ver el tráfico recibido primero en paquetes por segundos y en bits por Segundo.

De la tercera a la cuarta grafica podemos observar el comportamiento del nodo 1, observamos que las dos primeras se mantienen a 0 dado que esta estación envía tráfico, pero no recibe, observamos que las graficas del envío de datos, como era de esperar, coinciden con las graficas registradas por el escenario global.

Las últimas dos graficas se corresponden al registro de recepción de trafico por parte del nodo 2, como era de esperar también tiene el mismo aspecto que las graficas de envío del nodo 1 y las de recepción de trafico del escenario global.

5.2 Segundo escenario

En el momento de la implementación física de una red se ha de tener en cuenta la carga de tráfico que generan las aplicaciones que se van a utilizar. En una red empresarial existe tráfico de datos de aplicaciones, pero aparte de este tráfico hay aplicaciones que pueden generar trafico de voz o trafico de video (los tres en conjunto se denominan trafico multimedia). El objetivo parcial de este escenario es simular el tráfico de aplicaciones en una red inalámbrica y evaluando los resultados de la simulación poder decidir si la tecnología elegida para su

simulación es la correcta y si lo es ver hasta que limite se podría ampliar la red sin que el funcionamiento de esta se viera afectado.

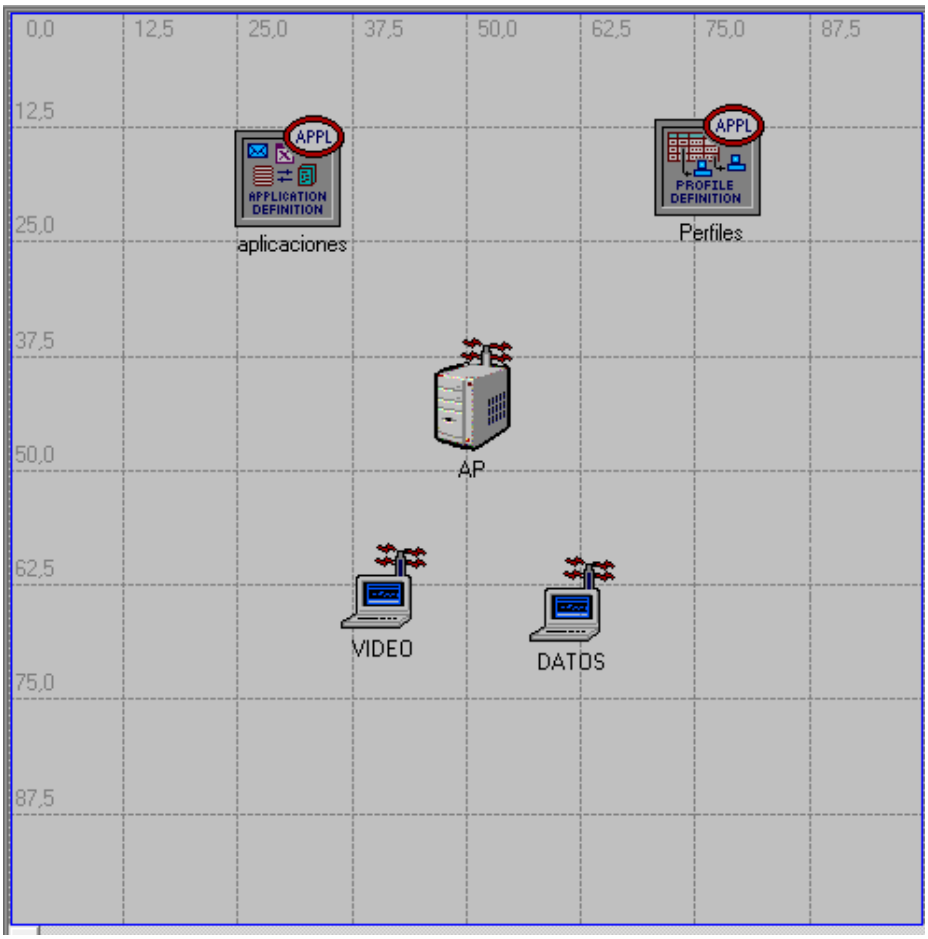
El propósito de este segundo escenario es experimentar como OPNET puede simular el tráfico propio de aplicaciones, en este caso solo utilizaremos dos tipos de aplicaciones distintas. Lo ideal hubiera sido hacerla con un número más elevado de aplicaciones y de estaciones, ya que así es como en un principio esto es lo que se da en la vida real, pero la restricción del software de edición académica me ha obligado a reducir a un número de 2 estaciones y 2 aplicaciones.

En el primer escenario utilizamos el software para verificar el correcto funcionamiento de la red. En este segundo vamos a hacer una evaluación de determinados parámetros básicos de la red que nos aportarán información esencial para su diseño físico.

A pesar de esta restricción el escenario es de sobra útil para ver como OPNET puede ser utilizado para la evaluación de escenarios con tráfico real de aplicaciones.

En esta ocasión simulamos una oficina de 100x100 (como en el primer escenario). Vamos a situar 2 estaciones WLAN que van a generar tráfico a aplicaciones de datos y video hacia el AP (Access Point).

El Access Point seleccionado es un servidor con capacidad inalámbrica que además de servir como nodo de comunicación nos servirá las aplicaciones mencionadas.

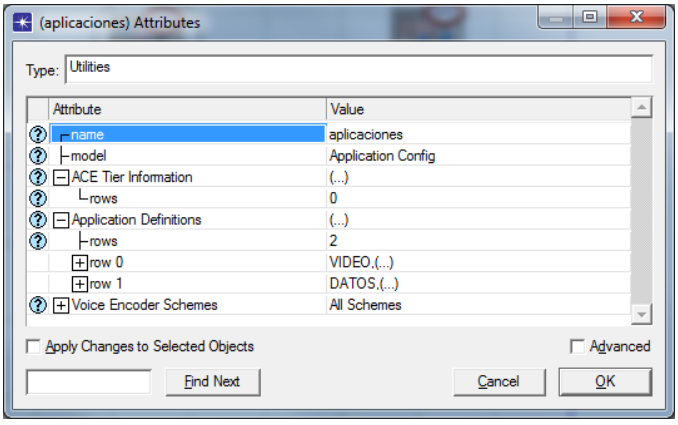


Configuración de aplicaciones:

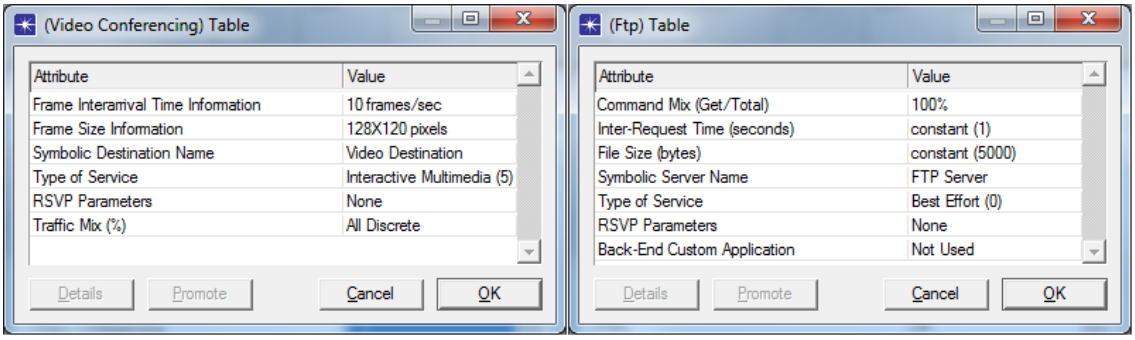
Application Configuration Object nos permite configurar una aplicación en común a un grupo de estaciones. Existen 8 aplicaciones por defecto.

Haciendo clic con el botón derecho podemos configurar sus atributos ->Edit Attributes.

Para definir las diferentes aplicaciones que utilizarán las estaciones pulsamos el elemento Aplication Config y seleccionas Edit Atributes. Definimos las aplicaciones DATOS y VIDEO cambiando el número de filas a 2.

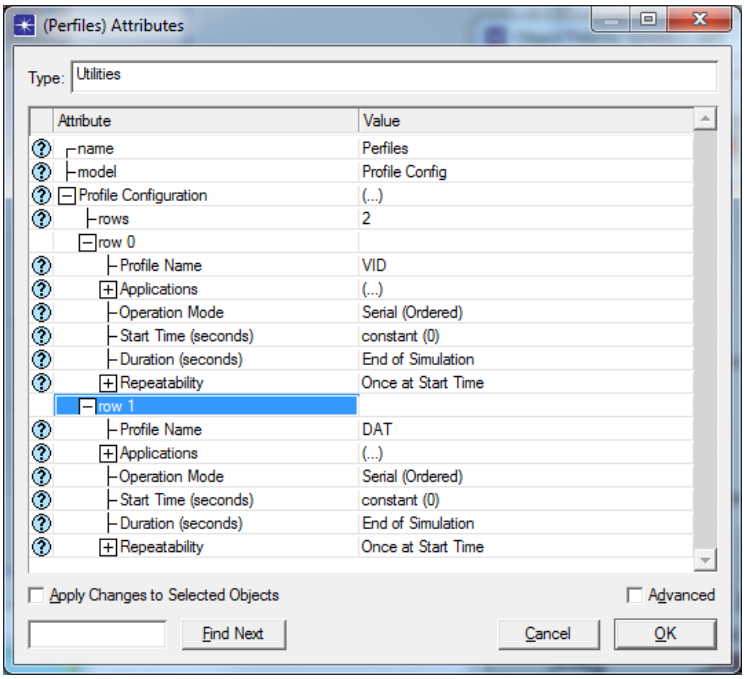


Tas ello configuramos las dos aplicaciones con los siguientes parámetros.



Configuración de perfiles

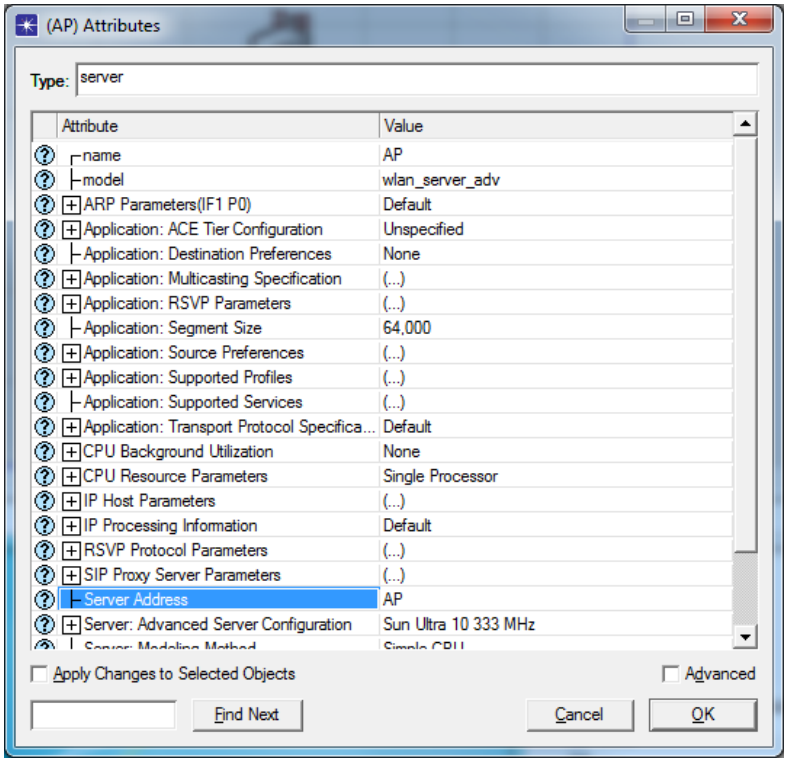
Para la configuración de perfiles seleccionamos *Profile Config* y al hacer clic con el botón derecho podemos editar sus atributos.



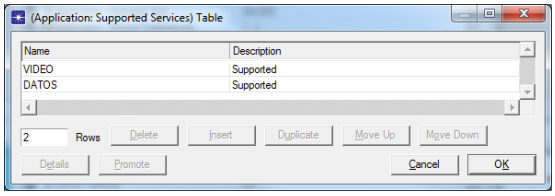
Todas las aplicaciones comienzan simultáneamente para ver claramente el comportamiento del entorno inalámbrico utilizando la priorización de servicios.

Configuración del punto de acceso

Es importante modificar el parámetro *Server Address*. Ya que define el nombre que le damos a nuestro punto de acceso para que las estaciones puedan conectarse a él.

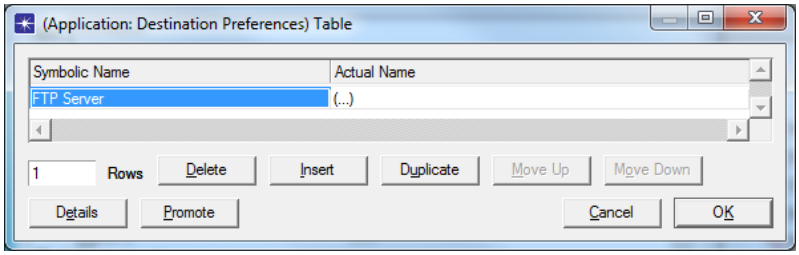


Añadimos las aplicaciones en el campo *Suported services*.

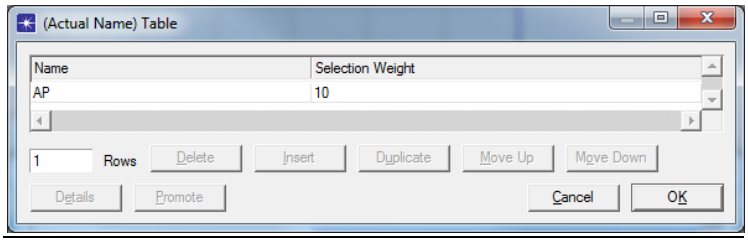


Configuración del punto de las estaciones

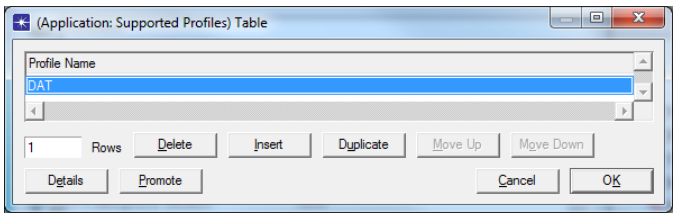
Configuramos las preferencias de destino de aplicación, *Applicarion:Destination Preferences*, añadiendo una línea para definir la aplicación utilizada por la estación.



Debemos introducir el nombre de la aplicación tal y como la definimos en *Aplication config*. Además para que envíe dicha aplicación al punto de acceso lo asignaremos en el campo *Actual name* .



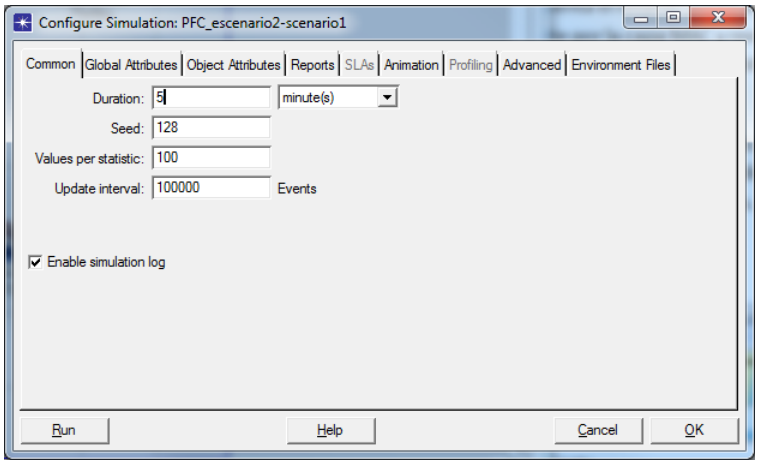
Ahora es necesario cambiar *Suported Profiles*, quedando de la forma siguiente:



Para la estación Video, la configuración es similar, teniendo en cuenta que en esta estación se configura la aplicación video.

Configuración de la simulación

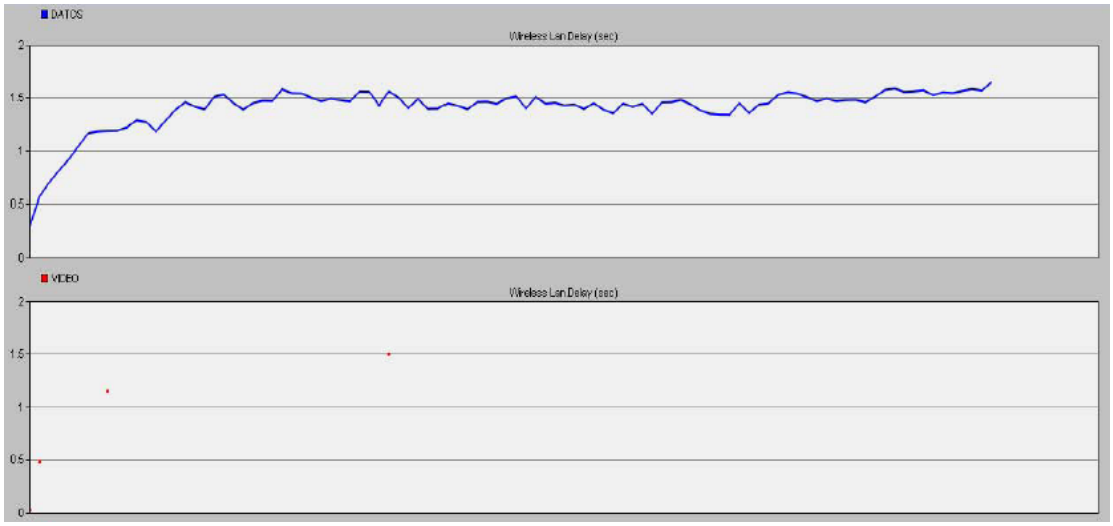
Configuramos una duración de la simulación de 5 minutos.



Parámetros a evaluar

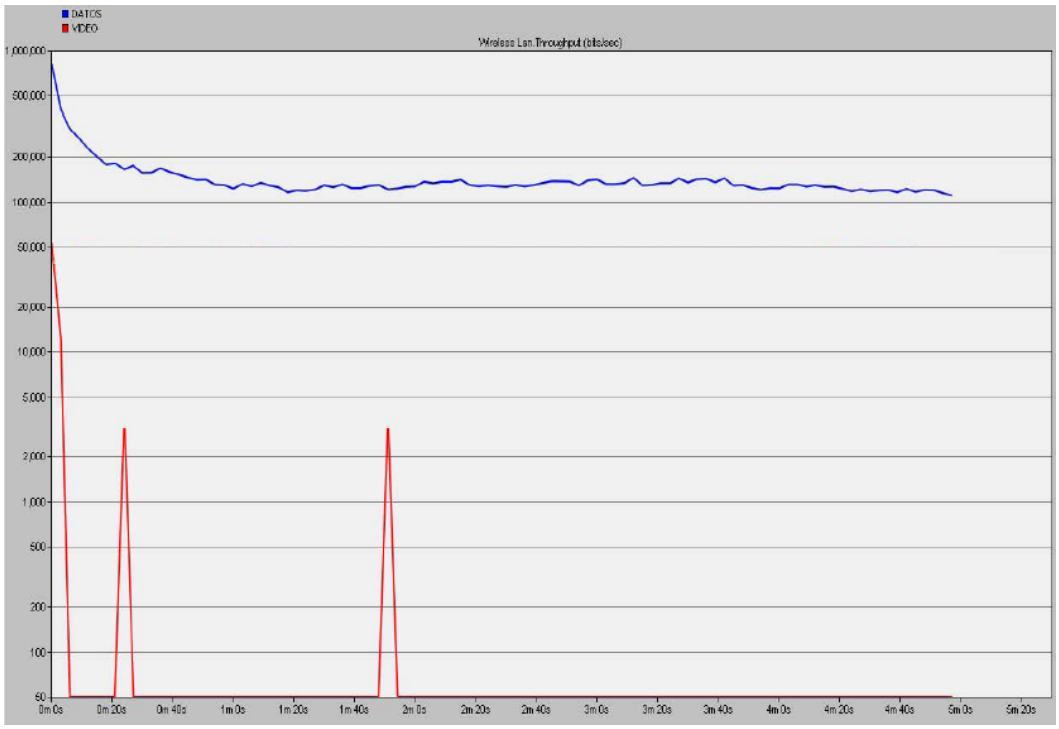
Retardo: Este parámetro representa el retardo punto a punto de todos los paquetes que han sido recibidos satisfactoriamente por la capa MAC y reenviados a la capa superior. Incluye los retardos por encolado y acceso al medio en la fuente MAC, recepción de todos los fragmentos individualmente y el retardo de la trama.

Observamos los resultados obtenidos de retardo para las 2 aplicaciones, siendo próximos al valor 1,5 segundos



Para una aplicación de datos lo podemos considerar un buen resultado dado que se transmite una gran cantidad de bytes en un tiempo relativamente aceptable y sobre una aplicación que no está condicionada por el retardo. Sin embargo, para aplicaciones de video este retardo sería muy grande ya que son aplicaciones que requieren asegurar un tiempo de acceso mínimo (los estándares ITU recomiendan un retardo máximo de 150 ms para aplicaciones de video interactivas).

Throughput: representa el tráfico total en bit/s recibido satisfactoriamente y reenviado a la capa superior. No incluye las tramas de datos unicast direccionadas de otra MAC, duplicidad de tramas antes de ser recibidas o tramas incompletas.



Se nos vuelve a hacer patente que la tasa de transmisión para el video sería fatal para una comunicación multimedia ya que daría lugar a múltiples errores y retardos en la comunicación.

Llegamos a la conclusión de que la tecnología inalámbrica tal y como se ha configurado no se podría implantar en una empresa que generara tráfico multimedia. La simulación se ha hecho con un mínimo de nodos y su resultado ha sido insatisfactorio. No tendría sentido ampliar la red en cuando a nodos y a tráficos, sólo la sobrecargaría más.

La versión completa OPNET Modeler incluye la posibilidad de simular otros mecanismos de acceso al medio como EDCA y HCCA que nos permiten reducir los retardos a través de la priorización de diversos tipos de paquetes de tráfico y mejorar la eficiencia del ancho de banda. A partir de un escenario mínimo (como el presentado) que funcionara correctamente podríamos ir añadiendo estaciones hasta ver cuál es el límite de la red y así en el momento de su implementación física tener garantías de que el diseño de red no fracasará.

6. Conclusiones

En este proyecto se ha pretendido realizar un estudio sobre la tecnología inalámbrica a la par que su simulación mediante el software OPNET. Existen muchos estudios sobre esta tecnología que actualmente se encuentra de moda y en pleno auge, en la cual se trabaja con ahínco en nuevas versiones que mejoren el estándar original.

OPNET es un producto líder en cuando a simulación de redes. En este proyecto hemos visto el modelado de una red simple entre dos equipos AD-HOC como punto de partida, y un escenario en el que se incluía tráfico de aplicaciones de datos y video.

A través de las simulaciones realizadas con la versión académica del software hemos comprobado el enorme potencial que supone el uso de este mecanismo sobre aplicaciones multimedia y la gran diferencia que supone su uso en parámetros fundamentales dentro de las comunicaciones como son el retardo y el througput, muy a tener en cuenta en la implementación física de las redes, ya que fallos en estos parámetros podrían hacer fracasar un diseño de red que en el momento de la implementación física conllevarían pérdidas de tiempo y dinero.

Dentro de la familia de productos OPNET he podido ver que existe una versión que se encarga específicamente de redes inalámbricas OPNET Modeller Windows suite, aunque la versión estándar del modeller y el IT Guru también nos proporcionan muchas posibilidades.

A pesar de las restricciones de la versión académica, queda presente la gran potencia de OPNET, a partir de un interfaz de creación de modelos muy intuitivo tanto en el momento de diseñar escenarios como en el momento de programar simulaciones de la red funcionando y la recolección de resultados para su posterior análisis.

7. Bibliografía

- Cisco Systems: Fundamentos de redes inalámbricas. Persom Prentice Hall (2006).
- Cisco systems: Guía oficial para el examen de certificación CCENT/CCNA ICND1. Persom Prentice Hall (2008).
- Matthew, Gast: 802.11 Wireless Networks: The Definitive Guide. O´Reilly (2005).
- Neil P. Reid, Ron Seide: 802.11 (wi-fi): Networking Handbook. McGraw-Hill/Osborne (2003).
- Alan Holt y Chi-yu Huang: 802.11 Wireless Networks: Security and Analysis. Springer (2010).
- Ohtrman Frank: WIMAX in 50 pages. Monnoz Publishing (2008).
- Fernando Andreu, Izaskun Pellejero, Amaia Lesta: Redes WLAN. Fundamentos y aplicaciones de seguridad. Marcombo (2006).
- Roldan, David: Comunicaciones Inalámbricas. RA-MA (2004).
- Huidobro Moya, Jose Manuel: Comunicaciones en Redes WLAN. Creaciones Copyright (2005).
- Raya, Jose Luis y Laura: Redes Locales (4ªED). RA-MA (2006).
- Muñoz Rodríguez, David: Sistemas inalámbricos de comunicación personal. Marcombo (2002).
- Klaus Wehrle, Mesut Günes y James Gross: Modeling and Tools for Network Simulation. Springer (2010).
- Zheng Lu and Hongji Yang: Unlocking the Power of OPNET Modeler. Cambridge University Press (2012).
- Jesse Russell, Ronald Cohn: OPNET. Book on Demand LTD (2012).
- Aboelela, Emad: Network Simulation Experiments Manual 3rd Edition. Morgan Kaufmann (2011).
- Adarshpal S. Sethi y Vasil Y. Hnatyshin: OPNET User Guide for Computer Network Simulation. Chapman and Hall/CRC (2012).

Páginas en internet:

- www.cisco.com
- www.opnet.com
- www.wikipedia.org
- www.riverbed.com
- www.mobitex.com
- www.ieee802.org
- www.bluetooth.com