Universidad Central "Marta Abreu" de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Incremento de la cantidad de usuarios de una red LAN usando WLAN

Autor: Abigail Rodríguez Alejo

Tutor: MSc. Roberto Carlos Álvarez Valdera

Santa Clara

2013

"Año 55 de la Revolución"

Universidad Central "Marta Abreu" de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

TRABAJO DE DIPLOMA

Incremento de la cantidad de usuarios de una red LAN usando WLAN

Autor: Abigail Rodríguez Alejo

E-mail: ralejo@uclv.edu.cu

Tutor: MSc. Roberto Carlos Álvarez Valdera

E-mail: roberto.alvarez@etecsa.cu

Santa Clara

2013

"Año 55 de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Automática, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Autor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

Hay una fuerza motriz más poderosa que el vapor, la electricidad y la energía atómica, la voluntad.

Albert Einstein.

DEDICATORIA

A mis padres por ser la luz que ha guiado mi camino, a mi familia por brindarme su apoyo en todo momento, a mi novia por estar siempre a mi lado y de manera especial a mi abuelo Rodríguez por haberme dado tan buenos consejos.

AGRADECIMIENTOS

- A mi tutor Roberto Carlos Álvarez Valdera por sus enseñanzas, su tiempo y su ayuda imprescindible en la realización de este trabajo.
- A mis padres y a mi novia por su apoyo incondicional.
- A mis Abuelas por el cariño que me han dado siempre.
- A mis tíos, a mis tías más queridas y a todos mis primos, por apoyarme en todo momento y mostrar siempre su confianza en mí, lo cual me ha dado fuerzas para seguir adelante.
- A mis abuelos que aunque no están presentes físicamente, yo se que estarían muy contentos en este momento.
- A mis amigos por haber convertido el grupo de estudio en una pequeña familia que estoy seguro que perdurará.
- A Carmen Álvarez y a su familia por estar dispuestos a ayudarme siempre.
- A Yudania por su colaboración en la tesis.
- A mis amigos del barrio, en especial a Yordano y Yansel.

TAREA TÉCNICA

- Búsqueda bibliográfica de trabajos sobre redes LAN y WLAN.
- Estudio de las características, ventajas, desventajas y estándares de las redes WLAN, así como los principales elementos a tener en cuenta en su implementación.
- Estudio de trabajos donde se simulen redes LAN y WLAN usando OPNET Modeler.
- Simular usando OPNET Modeler diferentes escenarios donde se incrementen la cantidad de usuarios de una red LAN usando WLAN.
- Análisis de los resultados basándose en los gráficos obtenidos de la simulación.

RESUMEN

Actualmente es común la utilización de las redes de área local inalámbricas (WLAN) en el incremento de la cantidad de usuarios de una LAN, pero si esto no se realiza de la manera correcta puede afectar el funcionamiento de la red. En este trabajo se presenta una reseña sobre el estado y desarrollo de las principales versiones del estándar IEEE 802.11. También se explican los principales elementos a tener en cuenta en la implementación de una WLAN como son: la correcta elección del protocolo de seguridad, la asignación de canales, la atenuación por obstáculos, entre otros. Se proponen diferentes escenarios donde se amplía una red LAN usando WLAN y se explica cómo configurar estos en el simulador de redes OPNET Modeler. Los parámetros seleccionados para realizar el análisis fueron: carga, demora, razón de transferencia y utilización del canal. Se demostró que los diferentes escenarios de expansión estudiados no sufrieron modificaciones que afectaran su funcionamiento, debido a que se comprobó que mientras hay suficiente ancho de banda disponible la demora no necesariamente se ve afectada por el incremento de los usuarios o de la carga. Los resultados obtenidos pueden servir de base para el análisis de redes con mayor complejidad.

TABLA DE CONTENIDOS

PENSAMIENTO i

DEDICATORIA ii

AGRADECIMIENTOS iii

TAREA TÉCNICA iv

RESUMEN v

INTRODUCCIÓN 1

Organización del informe 3

CAPÍTULO 1. ANÁLISIS DE LAS WLAN 4

1.1 Características generales de las WLAN 4

1.2 Aplicaciones, ventajas y desventajas de las WLAN 5

1.3 Estándares 802.11 6

1.3.1 IEEE 802.11 6

1.3.2 IEEE 802.11a 6

1.3.3 IEEE 802.11b 7

1.3.4 IEEE 802.11g 7

1.3.5 IEEE 802.11n 9

1.3.6 IEEE 802.11ac 10

1.4 Modos de operación de las redes inalámbricas 11

1.4.1 Redes Ad hoc 11

1.4.2 Modo infraestructura 12

1.5 Seguridad en redes WLAN 13

1.6 Elementos a tener en cuenta en la Implementación de una WLAN 16

1.6.1 Uso de la seguridad según las características de la WLAN 16

1.6.2 Puntos de Acceso en la implementación 17

1.6.3 Reglas de diseño y Consejos prácticos 20

1.7 Conclusiones parciales: 21

CAPÍTULO 2. EVALUACIÓN DE ESCENARIOS DE INTERCONEXIÓN DE REDES LAN CON WLAN 22

2.1 Ejemplos de escalabilidad de redes LAN usando WLAN. 22

2.2 Características de la red 26

2.3 Simuladores de redes 27

2.4 Características y ventajas del OPNET Modeler 28

2.5 Creación y representación de los Escenarios a simular 28

2.6 Configuración de las Aplicaciones y los Perfiles 32

2.6.1 Configuración de las aplicaciones 32

2.6.2 Configuración de los perfiles 33

2.7 Configuración de la LAN 35

2.7.1 Configuración del switch 36

2.7.2 Configuración de los servidores 36

2.7.3 Configuración de las PC cableadas 37

2.8 Configuración de la WLAN 39

2.8.1 Configuración de las PC inalámbrica 39

2.8.2 Configuración de los AP 41

2.9 Selección de las Estadísticas que se valorarán 41

2.10 Conclusiones parciales 43

CAPÍTULO 3. ANÁLISIS DEL COMPORTAMIENTO DE LOS PARÁMETROS DE LA RED..... 44

3.1 Análisis de la carga (load) 44

3.2 Análisis de los diferentes tipos Demora (Delay) en la red 47

3.2.1 Demora Ethernet (Ethernet delay) 47

3.2.2 Demora media de acceso (Media Acces Delay) 49

3.2.3 Demora en la WLAN (Wireless LAN delay) 49

3.2.4 Comparación de la demora Ethernet con la demora en la WLAN 50

3.3 Razón de transferencia (througput) y utilización del canal 51

3.3.1 Razón de transferencia (througput) 51

3.3.2 Utilización del canal 53

3.4 Conclusiones parciales 55

CONCLUSIONES Y RECOMENDACIONES 56

Conclusiones 56

Recomendaciones 57

REFERENCIAS BIBLIOGRÁFICAS 58

ANEXOS 61

Anexo I Definición de un nuevo proyecto 61

Anexo II Elementos utilizados en la creación de los escenarios 62

INTRODUCCIÓN

Las tecnologías inalámbricas tienen gran auge en la actualidad, además de ser las más prometedoras. Se desarrollan a diario nuevos estándares en la búsqueda de mayor velocidad de transmisión y niveles de seguridad más altos (Martinez, 2011). Tal ha sido el desarrollo de estas tecnologías que en un cuarto de siglo el número de usuarios pasó de unos pocos a la mitad de la población mundial (Katz and Fitzek, 2009). Entre estas tecnologías se encuentran las redes de área local inalámbricas (WLAN), las cuales son cada vez más importantes en las comunicaciones del mundo de hoy (Martinez, 2011). Estas juegan un papel fundamental en el desarrollo de empresas, universidades e industrias (Barrenechea Zavala, 2009). Las WLAN ofrecen varias ventajas que han favorecido este auge como son movilidad, bajo costo de instalación, escalabilidad entre otras (Summaries, 2003).

Hoy en día las WLAN se han podido expandir sin problemas de compatibilidad gracias a la creación por la IEEE (Institute of Electrical and Electronic Engineers) de un grupo de trabajo específico 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 (Romero Kanashiro, 2013).

El uso de una WLAN para incrementar la cantidad de usuarios de una red LAN trae consigo todas las ventajas mencionadas anteriormente, pero las WLAN tienen mayor demora que las redes LAN, además si no se tiene en cuenta el número de computadoras (PC) que se conectarán a esta, puede ocurrir un aumento del tráfico en la red que provoque un mal funcionamiento de la misma. Por todas estas razones es necesario hacer un estudio que permita conocer sobre las WLAN y su implementación. Además de realizar un análisis del comportamiento de las redes LAN y WLAN luego de interconectarse, usando para esto la herramienta de simulación OPNET Modeler, la cual permite conocer de manera

aproximada cuál será el comportamiento de los principales parámetros de la red, tales como demora (Delay), razón de transferencia (Throughput), carga (load) y utilización del canal, todo esto sin necesidad de realizar el montaje real de la misma.

Debido a lo anterior es que como situación del problema se plantea la siguiente interrogante:

¿Cómo resolver el incremento de la cantidad de usuarios en las redes LAN usando WLAN?

Para dar respuesta a la situación del problema planteado se propone como objetivo general de este trabajo: Desarrollar un procedimiento de actualización de una red LAN con la interconexión de una WLAN.

Y los siguientes objetivos específicos:

1. Realizar un estudio teórico de las características, ventajas, desventajas, estándares y seguridad de las redes WLAN, así como de los principales elementos a tener en cuenta para una correcta implementación.

2. Proponer diferentes escenarios donde se aumente el número de usuarios de una red LAN usando WLAN. Además de modelar y simular estos usando la herramienta de simulación OPNET Modeler

3. Analizar los resultados de las simulaciones para conocer el comportamiento de los principales parámetros de la red.

Con los resultados de esta investigación se espera contribuir en el entendimiento de las redes WLAN y en cómo implementar de la manera correcta esta tecnología. Además se muestra cómo simular en el OPNET Modeler varios escenarios con redes LAN interconectadas con WLAN y cómo analizar el resultado de estas simulaciones.

La culminación de este trabajo pondrá a disposición de los especialistas, investigadores y diseñadores de redes un material de consulta, que sirva de base para posibles investigaciones. Además puede servir de apoyo a la asignatura Modelación y Simulación de Redes.

Organización del informe

El informe de la investigación se estructura en introducción, capitulario, conclusiones, referencias bibliográficas y anexos.

En la introducción. Se recoge la importancia y necesidad de la realización de la investigación.

Capítulo 1 Análisis de las WLAN. Se abordan de manera concreta las principales versiones del estándar 802.11, en cuanto a sus características, ventajas y desventajas. Además se explican los principales elementos a tener en cuenta para una correcta implementación de una WLAN.

Capítulo 2 Evaluación de escenarios de interconexión de redes LAN con WLAN. Se proponen diferentes escenarios donde se incrementa la cantidad de usuarios de una red LAN usando WLAN y se explica cómo configurar y simular estos en OPNET Modeler.

Capítulo 3 Análisis del comportamiento de los principales parámetros de le red. Está dedicado al análisis de los diferentes resultados de la simulación.

Conclusiones: Se exponen los principales resultados obtenidos.

Referencias Bibliográficas: Se hace un listado de las distintas bibliografías consultadas siguiendo la metodología establecida para ello.

Anexos: Se incluyen temas que requieran ser tratados en el trabajo pero que por su tamaño y por no estar relacionado directamente con el tema propuesto no pudieron ser abordados en el capitulario.

CAPÍTULO 1. ANÁLISIS DE LAS WLAN

En los últimos años se ha visto una expansión rápida y exitosa de las tecnologías inalámbricas, lo que ha provocado que estas se conviertan en algo común en nuestras vidas, ejemplo en universidades, oficinas, aeropuertos, etc (Chávez, 2009). Entre estas se encuentran varias soluciones WLAN (Wireles Local Area Network) como son Bluetooth, Home RF (Home Radio Frecuencia) y Wi-Fi (IEEE 802.11) siendo esta última la que disfruta de un mayor respaldo (Álvarez Paliza, 2010). El protocolo IEEE 802.11 surge debido a la necesidad de los usuarios de las redes de área local (Local Area Network, LAN) de tener movilidad, además ofrece reducción en los costos, facilidad de instalación y adaptabilidad entre otras ventajas (Rosas Ramos, 2006).

En este capítulo se mencionan las principales características, ventajas y desventajas de las WLAN. Se abordan de manera concreta las principales versiones del estándar IEEE 802.11. Además se explican los principales elementos a tener en cuenta para una correcta implementación de una WLAN.

1.1 Características generales de las WLAN

Las Redes de Área Local Inalámbrica (WLAN) son sistemas de comunicaciones de datos flexibles que comúnmente se usan en el aumento de la escalabilidad de redes LAN o como alternativa a estas (Romero Kanashiro, 2013). Para la conexión se usa un medio inalámbrico como radio frecuencia o comunicaciones infrarrojas lo cual permite que el usuario remoto aunque no esté físicamente unido a la red se mantenga conectado a la misma (Rosas Ramos, 2006). Las WLAN tienen una cobertura cercana a los 100 metros lo cual hace que comúnmente se usen en oficinas, viviendas y centros estudiantiles (Ghetie, 2008), estas redes transmiten información en tiempo real (Romero Kanashiro, 2013) y

combinan la movilidad de los usuarios con la conectividad mediante una configuración sencilla, posibilitando de esta manera la existencia de las LAN móviles (Álvarez Paliza, 2010).

1.2 Aplicaciones, ventajas y desventajas de las WLAN

Las WLAN transmiten información en tiempo real a una terminal central y esto ha hecho que ganen importancia en campos como la manufactura, almacenes, etc., además son muy usadas en los hogares para compartir el acceso a internet entre computadores (Romero Kanashiro, 2013). También es común verlas en las oficinas y universidades (Chávez, 2009). Todas estas aplicaciones se benefician de las principales ventajas que ofrecen las WLAN como son (Summaries, 2003):

- Conexiones de red totalmente inalámbricas.
- Acceso a la red desde cualquier lugar de la instalación.
- Compatibilidad con redes cableadas.
- Son flexibles lo cual le permite adaptarse a cualquier entorno.
- Facilidad de instalación.
- Permite que los usuarios tengan movilidad.
- Escalabilidad.

Desventajas de las WLAN (Flores, 2009, Cartas, 2009):

- La calidad del servicio es menor que en las redes cableadas.
- Son redes muy sensibles a la interferencia.
- Tienen pérdidas de la señal debido a la trayectoria.
- Es vulnerable la seguridad de la red debido al medio de transmisión que no reconoce límites, aunque ya se han creado protocolos de seguridad que hacen más difíciles las penetraciones externas.

1.3 Estándares 802.11

Hoy en día las redes inalámbricas se han podido expandir sin problemas de compatibilidad en parte gracias a los estándares de la IEEE como es el caso del 802.11 donde se definió el uso del nivel físico y de enlace de datos de red, especificando sus normas de funcionamiento (Romero Kanashiro, 2013). Se han creado muchas versiones de este estándar y en este epígrafe se explican las versiones 802.11, 802.11a, 802.11b, 802.11g, 802.11n y 802.11ac, haciendo un mayor énfasis en la 802.11g debido a que se utiliza en las simulaciones del capítulo 2, también se aborda con mayor fuerza el estándar 802.11ac debido a su actualidad.

1.3.1 IEEE 802.11

En el año 1997 fue publicado el estándar IEEE 802.11 que es el estándar original de esta familia el cual operaba a velocidades de solo 1 o 2 Mbps (Rosas Ramos, 2006). El estándar IEEE 802.11 trabaja en la banda de frecuencia de 2.4 GHz y usa modulación de señal de Espectro Expandido por Secuencia Directa (DSSS) o de Espectro Expandido por Salto de Frecuencia (FHSS) (Ahmad, 2005), el método de acceso al medio que emplea es el de acceso múltiple por detección de portadora con evasión de colisiones (Carrier Sense Multiple Access whit Collision Avoidance, CSMA/CA) por lo que parte de la capacidad del canal se pierde para garantizar las transmisiones (Gibson, 2002).

Este estándar permitía tantas opciones que se hacía difícil garantizar la interoperabilidad dejando bastante libertad a los fabricantes. El mismo fue superado rápidamente por el 802.11b (Quobis, 2009).

1.3.2 IEEE 802.11a

En el año 1999 fue aprobado el estándar 802.11a, que en sus inicios solo fue utilizado en Japón y Estados unidos ya que no fue hasta el 2003 que se le otorgó la licencia para operar en Europa (Quobis, 2009). Este estándar trabaja en la banda de 5 GHz, el tipo de modulación que utiliza es Multiplexación por División de Frecuencias Ortogonales (Orthogonal Frequency Division Multiplexing, OFDM) tiene una velocidad máxima de 54 Mbps debido a que la razón de datos permitida es de 6, 9, 12, 18, 24, 36, 48, o 54Mbs para un espaciamiento del canal de 20 MHz, siendo obligatorio soportar 6, 12, y 24Mbs, para el caso de que sean 10MHz o 5MHz de espaciamiento del canal las razones de datos

antes mencionadas se reducen en la misma proporción que el espaciamiento del canal (Committee, 1999, Committee, 2007). El 802.11a cuenta con 12 canales tiene un throughput máximo de 31 Mbps y un rango máximo de 80 metros (Ghetie, 2008). Esta versión tiene menos interferencia, pero necesita que exista línea de vista. Esta tecnología no tuvo la misma aceptación que la basada en el 802.11b debido a que tenía un rango menor, no era compatible con los estándares existentes ya que estuvo limitada en Europa (Quobis, 2009).

1.3.3 IEEE 802.11b

El estándar 802.11b fue aprobado en el año 1999, trabaja en la banda de 2,4 GHz y es una extensión de la modulación DSSS usada por el estándar original, ofrece velocidades de 1, 2, 5.5 y 11 Mbps (Committee et al., 2000, Committee, 2007). En la práctica debido a las cabeceras de este método no era posible superar los 6 Mbps en TCP (Transmission Control Protocol o Protocolo de Control de Transmisión) y los 7 Mps en UDP (User Datagram Protocolo o Protocolo de datagrama de usuario) (Quobis, 2009). Se producen interferencias con hornos microondas, teléfonos inalámbricos y otros equipos que trabajen en la misma frecuencia (2.4 GHz) (Acero Palacios, 2007). Este estándar solo utiliza DSSS ya que este puede manejar mejor que FHSS las señales de baja intensidad. El estándar 802.11b es el primer estándar en cubrir el modo de funcionamiento Ad-Hoc y su principal ventaja con respecto al 802.11a es que puede cubrir grandes superficies con un menor número de puntos de acceso (Hemández-Serrano and Pegueroles, 2004). El reducido costo, el aumento de la velocidad y el ser una extensión de una modulación DSSS del estándar original logró un rápido aumento en la popularidad de este estándar (Rosas Ramos, 2006).

1.3.4 IEEE 802.11g

El estándar 802.11g fue aprobado en el año 2003 y opera a una velocidad máxima de 54 Mbps y a una razón máxima de datos de 24.7 Mbps. Trabaja en la misma banda de frecuencia (2.4 GHz) que 802.11b y es compatible con este. Este estándar tiene 3 canales habilitados al igual que el 802.11b y a diferencia del 802.11a que tiene 12 canales (Ghetie, 2008). El 802.11g usa modulación OFDM y CCK (Complementary Code Keying o Modulación por Código Complementario) con una razón de datos de 1, 2, 5.5, 11Mbps en CCK al igual que 802.11b y de 6, 9, 12, 18, 24, 36, 48, y 54 Mbps en OFDM esto permite

que 802.11g pueda elegir según sea conveniente en un mayor rango que el de 802.11a y el 802.11b (Escudero Pascual, 2009). En la siguiente figura se puede observar la razón de datos esperada para diferentes rangos.

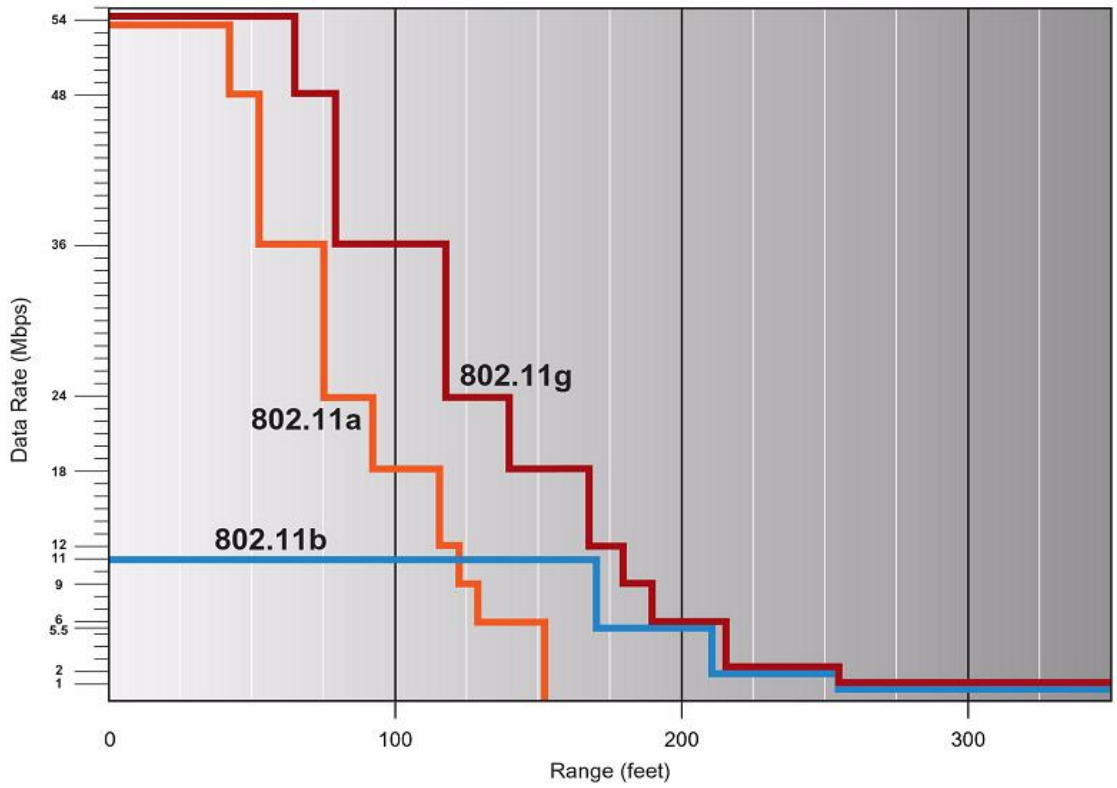


Figura 1.1. Razón de datos esperada a una distancia variable del punto de acceso de los estándares 802 .11a, 802.11b y 802.11g (Broadcom, 2003).

El estándar 802.11g alcanza los 100metros en interiores y hasta los 300metros en exteriores al igual que el 802.11b, mientras que el 802.11a alcanza 50 metros en interiores y 150 metros en exteriores, estos alcances máximos son teóricos debido a que en la práctica se ven afectados por interferencias electromagnéticas y por paredes u otro tipo de estructura (Flores, 2009). Aunque en el diseño de este estándar se tuvo en cuenta que fuera compatible con el 802.11b cuando el punto de acceso además de comunicarse con clientes 802.11g se comunica con clientes 802.11b se reduce significativamente la velocidad de transmisión (Romero Kanashiro, 2013). La aparición de chips y equipos tribanda, ha favorecido el aumento del uso de esta tecnología. Una característica adicional llamada SuperG permite duplicar la señal, pero en muchos caso afecta la compatibilidad con otros equipos (Quobis, 2009). El estándar 802.11g utiliza WPA (Wi-Fi Protected Access o

Acceso Wi-Fi protegido) como mecanismo de seguridad (Rosas Ramos, 2006). El estándar 802.11g llegó rápidamente al mercado incluso antes de su ratificación debido a que para construir equipos bajo este estándar se podían adaptar los ya diseñados para el estándar 802.11b (Romero Kanashiro, 2013). El estándar 802.11g demuestra una evolución en el estándar 802.11 y ha servido de base para el desarrollo de nuevos estándares que permiten mayor velocidad (Flores, 2009). En la tabla 1.1 se observa una comparación del estándar 802.11g con los que le precedieron.

Tabla 1.1. Características de los estándares 802.11/a/b/g

	802.11	802.11a	802.11b	802.11g
Año de aprobación	1997	1999	1999	2003
Frecuencia	2.4GHz	5GHz	2.4GHz	2.4GHz
Máxima razón de datos	2Mbps	54Mbps	11Mbps	54MBps
Modulación	DSSS y FHSS	OFDM	DSSS	OFDM y CCK
Razón de datos	1 y 2Mbps	6, 9 ,12 ,18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	CCK :1, 2, 5.5, 11 Mbps y OFDM: 6, 9, 12, 18, 24, 36, 48, 54Mbps

1.3.5 IEEE 802.11n

Hace 10 años la idea de Wi-Fi como principal tecnología de acceso al medio era casi un sueño, pero con el surgimiento del estándar 802.11n las WLAN se han establecido como una alternativa viable a Ethernet incluso para aplicaciones críticas para la misión (Aerohive, 2013). El estándar 802.11n fue aprobado por la IEEE en el año 2009, trabaja en las bandas de 2.4 y 5 Ghz ofreciendo velocidades de más de 100 Mbps (Committee, 2009). Este se construyó basándose en las versiones previas y se le añadió MIMO (Multiple Input, Multiple Output o Múltiple entrada múltiple salida), el cual utiliza múltiples transmisiones y antenas receptoras permitiendo incrementar el tráfico de datos (Romero Kanashiro, 2013). Este estándar tiene métodos mejorados de alta capacidad para solucionar el problema de la interferencia y de la fiabilidad necesaria para que Wi-Fi se convierta en una tecnología de infraestructura de capa base. Debido a la robustez del ancho de banda de las redes 802.11n el modelo resultante de control centralizado ya no puede ser considerado

como la mejor opción para estas redes puesto que mientras que los dispositivos de punto final reducen su complejidad desde un punto de vista de inteligencia de red la infraestructura de red debe aumentar la suya y automatizarse para asegurar que los dispositivos más simples no supongan un problema administrativo. El estándar 802.11n no es el punto final del aumento del rendimiento y la velocidad en las redes WLAN ya está a la vista el 802.11ac con promesas de hasta 1Gbps (Aerohive, 2013).

1.3.6 IEEE 802.11ac

El estándar 802.11ac aunque aún está a unos 3 o 5 años de un despliegue masivo debe estudiarse desde ahora en vista al alto impacto que tendrá en la arquitectura de red teniendo en cuenta el cambio en los patrones de tráfico de alta capacidad de la red (Aerohive, 2013).

Las principales mejoras de este estándar con respecto al 802.11n se pueden ver en la siguiente tabla.

Tabla 1.2. Mejoras del estándar 802.11ac sobre el 802.11n (Watson, 2012).

	IEEE 802.11n	**IEEE 802.11ac**
Frequency Band	2.4 GHz and 5 GHz	5 GHz only
Channel Widths	20.40 MHz	20.40, 80 MHz, 160MHz optional
Spatial Streams	1 to 4	1 to 8 total up to 4 per client
Multi-user MIMO	No	Yes
Single Stream (1x1) Maximun Client Data Rate	150 Mbps	450 Mbps
Three Stream (3x3) Maximun Client Data Rate	450 Mpbs	1.3 Gbps

El estándar 802.11ac opera solamente en la banda de 5 GHz la cual está más desocupada. Las mejoras más significativas de este estándar están en la capa física y entre ellas están: (Watson, 2012).

- Doblan el ancho de banda del canal y con esto doblan la razón de datos (Aerohive, 2013).
- El 802.11n solo permite 4 flujos espaciales mientras que 802.11ac permite un máximo de 8 flujos y cada flujo espacial adicional aumenta la razón de datos (Aerohive, 2013).

- MIMO multiusuario permitirá la transmisión simultánea de diferentes usuarios al mismo tiempo y en el mismo canal.
- La modulación se apoya en OFDM al igual que 802.11n y agrega 256 QAM (Quadrature amplitude modulation o Modulación de amplitud en cuadratura) que habilita más bit en el mismo tamaño del canal.

Se piensa que el estándar 802.11ac esté listo para finales del año 2013 aunque antes pueden aparecer dispositivos que cumplan las versiones provisionales del estándar (Lew, 2012).

1.4 Modos de operación de las redes inalámbricas

Los diferentes estándares 802.11 definen dos modos fundamentales para redes inalámbricas estos son Ad-hoc e infraestructura. Es importante entender que no siempre los modos se ven reflejados directamente en la topología debido a que por ejemplo un enlace punto a punto se puede implementar en modo ad hoc o Infraestructura. El modo se puede ver como la configuración individual de la tarjeta inalámbrica de un nodo, más que como una característica de toda una infraestructura (Buettrich and ESCUDERO, 2007).

1.4.1 Redes Ad hoc

Se le denomina red ad-hoc a un Conjunto de Servicios Básicos Independientes (IBSS) creado dinámicamente para el uso temporal. Esto se refiere a dos o más dispositivos interconectados entre sí de forma inalámbrica sin el uso de puntos de acceso ni de servidores (Baruch and Amitabh, 2008, Rosas Ramos, 2006). Para encaminar paquetes en este modo uno de los métodos básicos es tratar todos los nodos que conforman la red como un router y utilizar entre ellos un protocolo convencional (ejemplo los basados en el vector de distancia) para encaminarlos hacia su destino (Acero Palacios, 2007). En este modo para que dos estaciones puedan comunicarse tienen que verse mutuamente es decir que cada una esté en el rango de cobertura de la otra (Ahmad, 2005).

Las redes ad-hoc son fáciles y rápidas de instalar debido a su baja dependencia de la infraestructura, además la administración de estas no representa un problema. Todo esto contribuye en su bajo costo (Baruch and Amitabh, 2008). Estas ventajas son aprovechadas por ejemplo para conectar sistemas portátiles dentro de un salón de conferencia y de esta manera comunicarse durante el tiempo de una reunión. Este modo de operación tiene

inconvenientes como son su alcance limitado, la no integración en estructuras LAN existentes y el número de usuarios limitados (Quednow M, 2006).

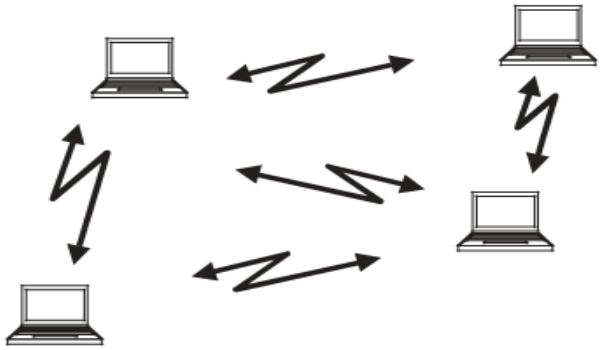


Figura 1.2. Red en modo ad-hoc (Ahmad, 2005).

1.4.2 Modo infraestructura

En el modo infraestructura existe un elemento de coordinación llamado punto de acceso o estación base. En este las estaciones inalámbricas pueden acceder a la red cableada si el punto de acceso se conecta a esta (Ahmad, 2005).

Configurando el Punto de Acceso (AP: Access Point) se logra una mayor cobertura de la red lo que permite que los usuarios tengan conexión a una mayor distancia, un AP en lugares abiertos tienen un alcance aproximado de 150 metros. Para el caso de zonas de mayor extensión se configuran más puntos de acceso y los usuarios se mueven de un AP a otro sin perder la conexión (roaming) (Espinosa Giraldo, 2011).

El modo infraestructura al usar AP permite emplear de manera óptima el tiempo de transmisión disponible en la red inalámbrica además ofrece otras ventajas como por ejemplo (Quednow M, 2006):

- las estaciones que no pueden "verse" directamente entre sí se pueden comunicar.
- permite una integración simple con estructuras cableadas ya existentes.

Entre sus desventajas está el mayor costo de los equipos y la mayor complejidad de la instalación y la configuración (Quednow M, 2006).

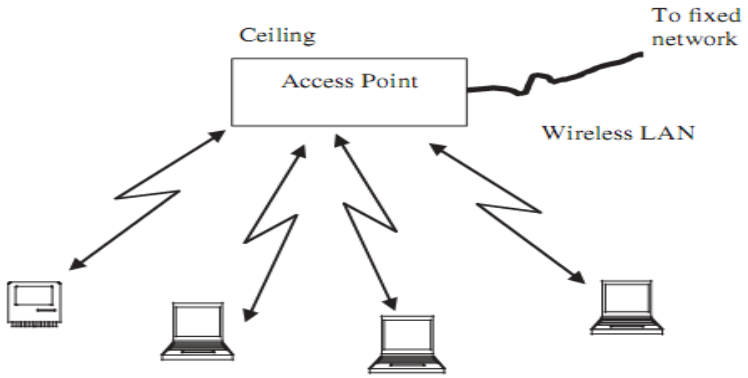


Figura 1.3. Red en modo infraestructura (Ahmad, 2005).

1.5 Seguridad en redes WLAN

Todos los sistemas de comunicación enfrentan algún grado de riesgos de seguridad. En el caso de las WLAN debido a la utilización para la conexión de un medio inalámbrico como la Radio Frecuencia (RF) este riesgo es mayor. Existen cuatro aspectos claves que deben ser parte de cualquier política de seguridad que abarque dispositivos móviles y puntos de acceso estos son: Autentificación, Autorización, Control de Acceso y Privacidad los cuales se explican brevemente a continuación (Ghetie, 2008):

Autentificación: Es para determinar la identidad de los usuarios y de esta manera solo los que estén previamente autentificados podrán acceder a los sistemas y servicios (Ghetie, 2008).

Autorización: Se comprueba generalmente mediante una base de datos remota si la entidad está autorizada para usar un determinado servicio. La autorización asume que una entidad ya ha ganado el acceso a uno de los recursos (Ghetie, 2008).

Control de Acceso: Generalmente son listas basadas en direcciones MAC (Media Access Control o Dirección de Control de Acceso al Medio) que indican los usuarios o computadoras que tienen disponible determinados servicios, estas listas son vulnerables y en las redes más grandes representan un dolor de cabeza administrativo (Ghetie, 2008).

Privacidad: Se protege la información mediante la encriptación de la transmisión y así se evita la captura de esta. Se parte de suponer que el remitente y el receptor conocen la llave para encriptar y desencriptar la información (Ghetie, 2008).

Se han utilizado varias soluciones de seguridad Wi-Fi de estas las más antiguas son: WEP (Wired Equivalent Privacy o Privacidad Equivalente a Cableado) (a 64, 128 y 256 bit), Shared Key Authentication y Filtros por IP o por MAC. Todas estas son vulnerables (Martinez, 2011).

WEP: Tiene como objetivo proporcionar confidencialidad a través del algoritmo de cifrado RC4 y prevenir el acceso desautorizado a la red inalámbrica a través de la autenticación con clave pre-compartida (Pre Shared Key, PSK). La encriptación con RC4 originalmente era de 40bit pero la IEEE introdujo una de 128 bit para hacerla más robusta lo cual no se pudo lograr de la manera deseada (Communications, 2008). Entre sus inconvenientes está que utiliza una misma clave simétrica y estática tanto en las estaciones como en el punto de acceso. Además las claves tienen que ser cambiadas de manera manual por los administradores de red lo cual provoca que en la mayoría de las ocasiones la claves se cambien poco o nunca (Amado Giménez, 2008). WEP proporciona una confidencialidad subjetivamente equivalente a la de una red LAN alambrada medio este que no emplea las técnicas de criptografía para reforzar la privacidad (Committee, 2005).

Filtrado de direcciones MAC (Media Access Control): Es una solución rudimentaria y muy poco segura, en estas se configuran los puntos de acceso con un listado de los dispositivos que están autorizados a conectarse a la red (Barrenechea Zavala, 2009).

Entre las soluciones actuales para la seguridad Wi-Fi están: Portales cautivos, 802.1x, WPA (Wifi Protected Access), 802.11i (WPA 2) (Martinez, 2011).

Portales cautivos: Es un sistema de validación de clientes para nodos inalámbricos que en dependencia del tipo de usuario asigna ancho de banda y da acceso a servicios diferentes (Martinez, 2011).

802.1x: Fue creado inicialmente por la IEEE para redes de área local alambrada y ha extendido su uso a redes inalámbricas. Es un protocolo de control de acceso y autenticación basado en la arquitectura cliente servidor, que restringe la conexión de equipos no autorizados a la red. La autenticación del cliente se realiza mediante el protocolo EAP (Extensible Authentication Protocol o Proceso de Intercambio de Autenticación) y el servicio RADIUS (Remote Authentication Dial-In User Service). En las redes inalámbricas cuando la estación de trabajo se asocia a un punto de acceso comienza el proceso. En ese

momento, la interfaz de red lo único que admite es el tráfico EAPOL (EAP over LAN), que es el requerido para efectuar la autenticación (Barrenechea Zavala, 2009).

WPA (WiFi Protected Access): Fue introducido por WiFi Alliance en el año 2002, está basada en un borrador de la norma 802.11i, que fue concebida para resolver los problemas encontrados en WEP con el objetivo de apresurar la introducción de un esquema de seguridad de redes WLAN más adecuado para el mercado empresarial. Para dar solución al problema de cifrado de WEP, introduce el protocolo para cifrado TKIP (Temporary Key Integrity Protocol) (Communications, 2008) . TKIP usa RC4 para realizar la encriptación al igual que WEP pero a diferencia de esta cambia la clave compartida entre punto de acceso y cliente cada cierto tiempo. Esto proporciona un método de distribución dinámico que refuerza significativamente la seguridad de la red (Gayal and Manickam, 2003). WPA emplea como mecanismo de autenticación el 802.1x y EAP. La norma WPA es de obligatorio cumplimiento para todos los miembros de la WiFi Alliance desde finales del 2003 (Barrenechea Zavala, 2009). WPA tiene un inconveniente y es que necesita una mayor infraestructura por ejemplo un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad (Maldonado Erazo, 2009).

80.11i (WPA 2): En el año 2004 WiFi Alliance actualizó la especificación WPA reemplazando la encriptación RC4 con la norma de seguridad avanzada AES (Advanced Encryption Standard) llamándole ahora WPA 2 (Communications, 2008). WPA 2 se diseñó utilizando la versión final del estándar 802.11i. Este representa una mejora significativa con respecto a las primeras normas de seguridad debido a que la norma de seguridad avanzada (AES) garantiza en principio que la información esté encriptada y que no pueda ser modificada por alguien que la intercepte (Amado Giménez, 2008). El cifrado AES es un algoritmo de cifrado en bloque con claves de 128 bits mientras que RC4 que es el utilizado en WEP es de flujo. WPA 2 necesita un hardware potente para realizar sus algoritmos y debido a esto los dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WAP 2. Para asegurar la integridad y autenticidad de los mensajes WPA 2 emplea CCMP (Counter-Mode/Cipher Block Chaining/Message Authentication Code Protocol) en lugar de los códigos MIC (Message Integrity Code o código de integridad del mensaje). Otra mejora de WPA 2 es que soporta el modo IBSS además del BSS (Basic

Service Set o Conjunto de Servicios Básicos) que era el único que soportaba WPA (Maldonado Erazo, 2009).

1.6 Elementos a tener en cuenta en la Implementación de una WLAN

En la implementación de una WLAN cuyo objetivo es incrementar la cantidad de usuarios de una red LAN, entre los aspectos más importantes a considerar están los relacionados con la seguridad y con los puntos de acceso. Además es conveniente conocer algunas reglas de diseño y tener en cuenta varios consejos prácticos. Debido a lo mencionado anteriormente en este epígrafe se abordan todos estos temas.

1.6.1 Uso de la seguridad según las características de la WLAN

En el epigrafe 1.5 se abordaron varias soluciones de seguridad para WLAN. La implementación de estas soluciones depende de si es una red nueva o no, de la importacia que tenga la información que se transporta por la red, del presupuesto con que se cuenta para llevar a cabo la implementacion y de otros elementos (Martinez, 2011).

La limitación del acceso mediante direcciones MAC no es suficiente para ninguna red debido a que un simple sofware analizador de redes permite ver las direcciones MAC de los clientes y robarlas, esto pasa principalmente en el protocolo 802.11b/g porque este no cifra las tramas (Mendigaña Castillo and Reina Ascencio, 2008).

El uso de WEP con clave estática es el mínimo nivel de protección que se le puede dar a una red, el cual puede ser suficiente en una red casera, pero no en una empresa, donde está formalmente desaconsejado debido a que en los entornos con un alto tráfico se pueden romper con facilidad las claves WEP de cualquier tarjeta (Martinez, 2011).

Las VPN (Virtual Private Networks o Red Privada Virtual) que en la mayoría de los servicios utilizan IPSEC (Internet Protocol security) que es un protocolo de la IETF (Internet Engineering Task Force o Fuerza de Tareas de Ingeniería de Internet) para apoyar el intercambio seguro de paquetes sobre el Protocolo de Internet (IP) (Rosas Ramos, 2006). Son una alternativa a tener en cuenta cuando ya existe una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x. Esta conlleva la instalación de uno o varios servidores que manejen las tareas de autenticación, cifrado de datos, y autorización de acceso además el cliente necesita software específico (Martinez, 2011).

En WPA para autenticar las estaciones existen 2 modos diferentes y el uso de uno u otro depende del entorno de aplicación. Estos son WPA-PSK (Wifi Protected Access-Pre Shared Key) o WPA EAP (Wifi Protected Access Extensible Auntentication Protocol). En entornos personales como pequeños comercios y casas se utiliza WPA con clave pre-compartida (WPA-PSK) y autenticación IEEE 802.1x. En estas circunstancias WPA se ejecuta en un modo especial conocido como ¨Home Mode ¨ o PSK (Pre Shared Key) el cual permite utilizar claves configuradas manualmente facilitando de esta forma el proceso de configuración para el usuario doméstico. En entornos empresariales debido a los estrictos requerimientos de cifrado y autenticación es más apropiado utilizar WPA con los mecanismos de IEEE 802.1x y el protocolo de autenticación extensible EAP que cuenta con procedimientos de gestión de claves dinámicos (Amado Giménez, 2008).

Aplicar 802.1x y EAP es la opción correcta si se desea montar una nueva red, o si los equipos de la red inalámbrica existente se pueden actualizar. Se pueden utilizar las soluciones WEP con clave dinámica, o la de WPA; debido a que ambas ofrecen un excelente grado de protección (Martinez, 2011).

1.6.2 Puntos de Acceso en la implementación

En este sub-epígrafe se explica lo relacionado con los puntos de acceso (AP) en la implementación de una WLAN. Se aborda específicamente la ubicación de los AP y la cantidad, así como otros aspectos.

Ubicación de los Puntos de Acceso

Los puntos de acceso deben colocarse en un punto en el que puedan cubrir toda el área donde se encuentran las estaciones. Con el objetivo de lograr una mejor cobertura la antena del repetidor puede colocarse a la altura del techo para evitar interferencias debido a los obstáculos.

Existen otras consideraciones a tener en cuenta para la ubicación de los puntos de acceso y estas son:

Atenuación por obstáculos

La atenuación por obstáculos debe tenerse en cuenta debido a que puede llegar a crear zonas de sombra dentro del área que se desea cubrir dificultando el paso de las ondas

electromagnéticas y a su vez crean atenuaciones y reflexiones considerables que afectan el diseño y desempeño de la red en ambientes interiores. Para que se tenga una idea de las afectaciones que pueden provocar los diferentes obstáculos en la siguiente tabla se mencionan los tipos de obstáculos y la atenuación que estos producen (Flores, 2009).

Tabla 1.3. Atenuación de Materiales a 2.4GHz (Flores, 2009).

Tipo de obstáculo	Atenuación
Tipo 1: Mampara de materiales sintéticos o de madera con un grosor de 2 o 3 cm	8.1 dB
Tipo 2: Paredes de 4 o 5 cm de grosor. Materiales sintéticos, madera o yeso.	13.0 dB
Tipo 3: Paredes de entre 10 y 15 cm de grosor de yeso, ladrillos y baldosas.	20.9 dB
Tipo 4: Paredes de entre 30 y 60 cm de grosor de yeso, ladrillo y cemento.	32.8 dB
Vidrios: Se incluyen ventanas y puertas de vidrio	19.2 dB
Metales: Ascensor, las puertas y las estanterías metálicas	32.25 dB

Asignación de canales

En la banda de 2.4 y 5GHz donde trabajan entre otros los estándares 802.11b y 802.11g se definieron 11 canales utilizables por equipos Wi-Fi, que pueden configurarse según las necesidades particulares. Estos canales no son completamente independientes y debido a esto los canales contiguos se superponen y se producen interferencias. Por esto se hace necesario una correcta asignación de los canales para permitir tener AP continuos sin traslaparse o interferir señales entre ellos. En la práctica solo es posible utilizar en forma simultánea 3 canales (1, 6 y 11). Esto es así en Estados Unidos y en muchos países de América, pero en Europa el **ETSI (**European Telecommunications Standards Institute o Instituto Europeo de Normas de Telecomunicaciones**)** ha definido 13 canales y por ejemplo para el caso de España, se pueden utilizar 4 canales no-adyacentes (1, 5, 9 y 13) (Barrenechea Zavala, 2009).

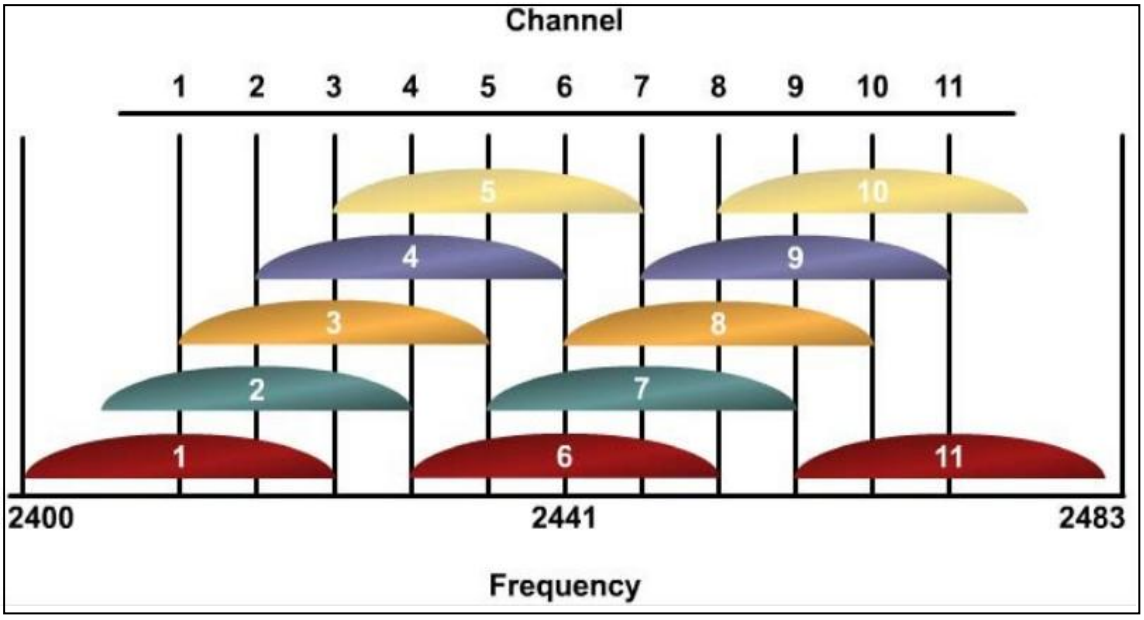


Figura1.4. canales sin interferencia en 802.11b (Cabrera E, 2007).

Comúnmente la asignación de canales se realiza solamente en los AP debido a que los "clientes" detectan automáticamente el canal excepto en los casos en que se forma una red "Ad-Hoc" o punto a punto cuando no existe AP (Barrenechea Zavala, 2009).

Roaming o movilidad

Es la capacidad de una estación móvil de desplazarse de una celda BSS a otra sin perder la conexión (Álvarez Paliza, 2010).

El Roaming se logra configurando varios AP en una red ESS (Extended Service Set o Conjunto de Servicios Extendidos) de forma tal que no se pierda el servicio. Se configuran varios AP como bridges y se conectan a la misma subred física (Todos los AP tienen un mismo router). Para lograr un desempeño óptimo se configura la densidad del AP como Low (bajo), Medium (medio), High (alto), en dependencia de a qué distancia están uno de otro. Por ejemplo en un área con alta densidad de usuarios donde los AP se encuentran cerca unos de otros se debe configurar la densidad en High lo cual permite un mayor ancho de banda debido a que fuerza a la estación móvil a buscar un nuevo AP si se baja de 11Mbps. La relación aproximada es que para una distancia máxima entre AP de 30m, 60m y 120m se configure la densidad en High, Medium y Low respectivamente (Cañas, 2004).

Teniendo en cuenta todo lo mencionado anteriormente se comprende que la ubicación de los puntos de Acceso no puede ser obra del azar si no de un proceso bien elaborado debido a que estas ubicaciones influyen en el funcionamiento y aprovechamiento de la red.

Determinación del número de AP (Flores, 2009)

En la determinación del número de AP influyen varios elementos como son el número de usuarios que se tendrá en cada área, las características de los equipos, la cobertura de estos y la capacidad de los equipos en la reutilización de frecuencias. También se tiene en cuenta la velocidad mínima que se dará a un usuario que está en el área de cobertura de un AP.

En la práctica el área de cobertura de los puntos de acceso no siempre es la que se indica en las hojas de datos, debido a que en estas aparecen estimaciones de alcance, basadas en condiciones ideales, es por esto que al variar las características de los lugares varía el alcance de los AP, por lo que no bastará con incrementar la potencia o la ganancia de los puntos de acceso para aumentar el área de cobertura de los mismos, puesto que algunos materiales presentan gran resistencia al paso de las ondas electromagnéticas.

Teniendo en cuenta lo mencionado anteriormente es necesario hacer un análisis profundo del lugar específico en que se instalará la WLAN y considerar elementos como el número de paredes su espesor, los techos y otros objetos debido a que estos pueden impedir el paso de la señal inalámbrica y de esta manera provocar un efecto negativo en el rango.

Actualmente existen equipos que entre sus especificaciones técnicas, garantizan un radio de cobertura de más de 200 metros en ambientes exteriores, y más de 100 metros en ambientes interiores.

1.6.3 Reglas de diseño y Consejos prácticos

Algunas reglas de diseño (Cañas, 2004):

- Espaciar lo máximo posible los AP sin que se pierda la cobertura de toda el área. Emplear este criterio contribuye a reducir la interferencia co-canal, costos de equipo e instalación.
- Para redes de un solo piso usar los canales 1, 6 y 11 para evitar toda interferencia inter-canal.

- Para redes de varios pisos emplear los canales: 1, 4, 7 y 11 para limitar la interferencia inter-canal.

Para el diseño de una WLAN se debe tener en cuenta todo lo expresado en este epígrafe sobre seguridad y AP. Además de los consejos prácticos que se mencionan a continuación.

Consejos prácticos (Cañas, 2004):

- No ubicar los AP en lugares inaccesibles.
- En vez de usar un AP con amplificador de potencia es mejor utilizar varios con baja potencia lo cual permite mayor cobertura.
- Seleccionar un AP con opción de antena externa.
- Evitar mezclas de AP debido a que se hace más difícil la estimación de celdas, además se dificulta la actualización del software y la optimización por parametrización de la red.

Breve descripción del procedimiento de diseño: Inicialmente se ubican los AP luego se ajustan estas ubicaciones basándose en mediciones de intensidad de señal. Se construye un mapa de cobertura y teniendo en cuenta este se le asigna canales a los AP. Se debe considerar que si se cambia la ubicación de un AP todo el volumen se mueve. Si hay varios AP, el traslape debe ser mínimo.

1.7 Conclusiones parciales:

Se determinó que durante los próximos años se seguirá incrementando el uso de las WLAN gracias a las ventajas que ofrecen desde sus inicios como movilidad, facilidad de instalación, entre otras, además del surgimiento de estándares como el IEEE 802.11ac que promete velocidades de hasta 1Gbps. Se llegó a la conclusión de que para entornos empresariales, se debe utilizar el protocolo de seguridad WPA con los mecanismos de IEEE 802.1x y el protocolo de autenticación extensible EAP que cuenta con procedimientos de gestión de claves dinámicos. Se definieron seguridad, atenuación por obstáculos, Roaming y la asignación de canales como los principales elementos a tener en cuenta en la implementación de una WLAN.

CAPÍTULO 2. EVALUACIÓN DE ESCENARIOS DE INTERCONEXIÓN DE REDES LAN CON WLAN

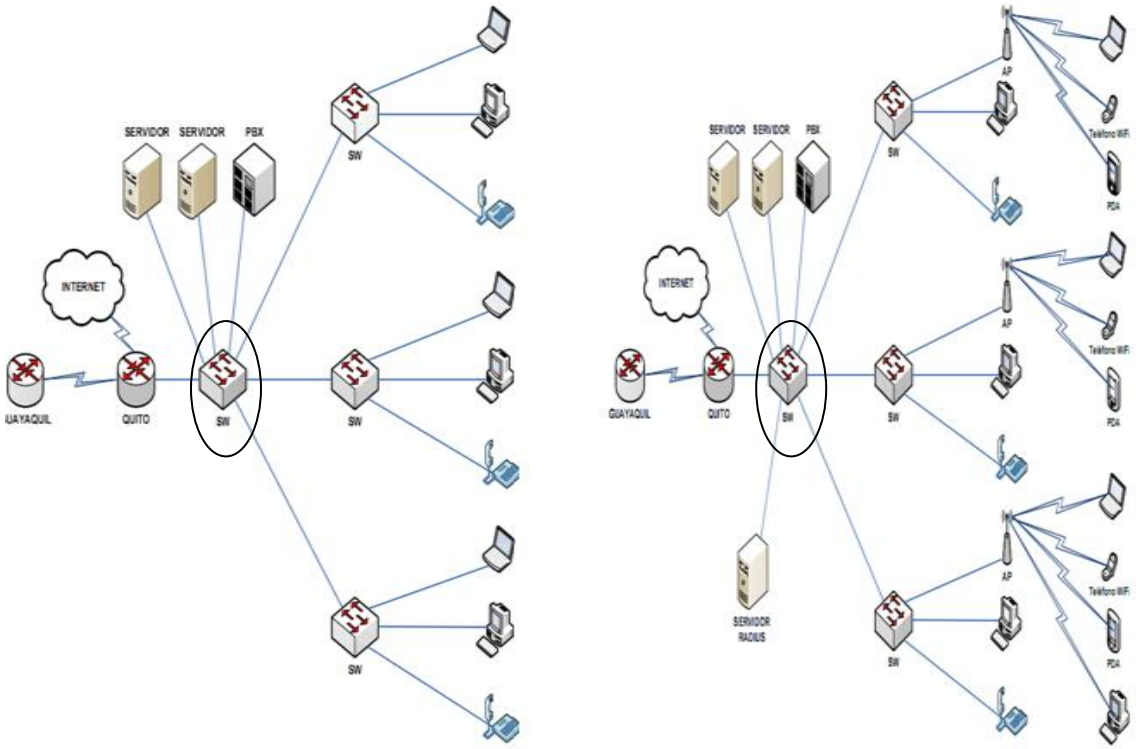
En este capítulo se analizan algunos proyectos relacionados con el incremento de la cantidad de usuarios de una red LAN usando WLAN. También se explican las posibilidades que brindan los simuladores de redes, en especial el OPNET Modeler (OPtimized Network Engineering Tools) y como parte fundamental del capítulo se representan los diferentes escenarios, así como la configuración de estos en el OPNET Modeler.

2.1 Ejemplos de escalabilidad de redes LAN usando WLAN.

En este epígrafe se muestran tres ejemplos donde se aumenta la escalabilidad de una red LAN usando WLAN, en los cuales se observa el modo de operación usado, la topología, los estándares y demás elementos que puedan ser de interés para este trabajo.

Primer Ejemplo (Flores, 2009)

Este tiene como objetivo aumentar la escalabilidad de la red de la empresa Bio-Electrónica Blanco, mediante la conexión de equipos inalámbricos usando WLAN.



a) **b)**

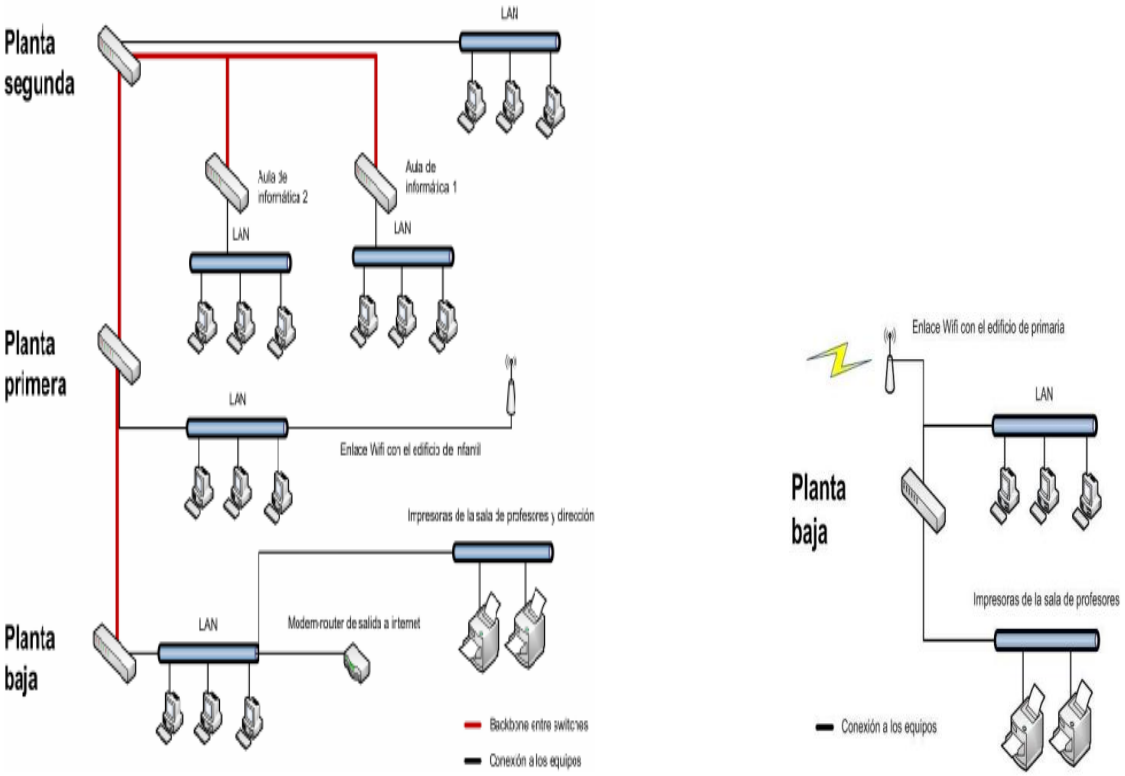
Figura 2.1. Red de la empresa Bio-Electrónica Blanco a) antes del aumento de escalabilidad, b) después del aumento de escalabilidad.

En la figura 2.1 se puede observar que la red de la empresa presenta una topología tipo estrella, esta tiene como punto central un switch, marcado con un círculo en la figura 2. 1 a y b, el cual se conecta a la red LAN. En este caso los tipos de tráfico que se transportan a través de la red son: Voz y Datos a través de Internet, Acceso a Internet y Correo electrónico, Bases de datos y Transferencia de archivos, Servicios de video sobre IP, Otros Servicios (impresión, escáner, servicio de fax). El estándar que se utiliza en este trabajo es el IEEE 802.11g, el cual se explica en el capítulo 1 en el sub-epígrafe 1.3.4, podemos destacar que opera hasta 54 Mbps y trabaja en la banda de 2.4GHz.

Segundo Ejemplo (Merinero, 2010)

Este tiene como objetivo unir las redes LAN de dos edificios separados aproximadamente 150 metros, mediante un enlace Wi-Fi. La red está dividida físicamente en dos partes, una

en el edificio donde hay una escuela primaria y la otra donde hay un círculo infantil. Figura 2.2.



a) **b)**

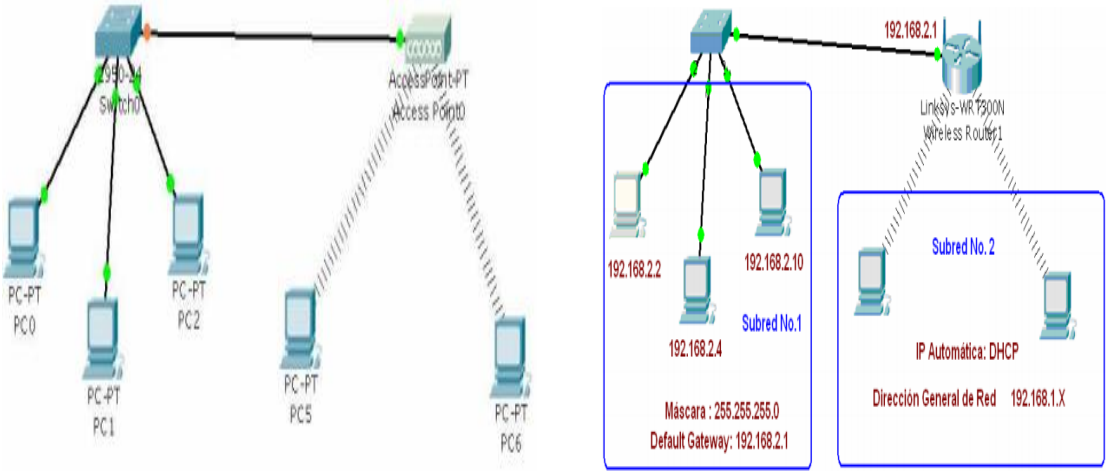
Figura 2.2. Distribución general de la red a) escuela primaria, b) circulo infantil.

El cable rojo que se muestra en la figura 2.2 a) es un troncal o backbone que une todos los switches de las plantas del edificio. Por otra parte los puntos de red de cada planta se unen a su switch correspondiente en esa misma planta mediante una topología de estrella. En esta red utilizan para el cableado el estándar Gigabit Ethernet. Para unir ambos edificio se emplea un enlace Wi-Fi en modo WDS (Wireless Distribution System o Sistema de Distribución Inalámbrico), sin posibilidad de admitir más clientes porque de otro modo no estaría disponible el cifrado WPA2-PSK que en este caso interesa para garantizar la seguridad del enlace, además no tiene sentido admitir más clientes ya que se trata de antenas direccionales que se usan para unir dos localizaciones. El enlace Wi-Fi fue necesario debido a que la separación entre los edificio supera los 100 metros , el costo es menor que el de la fibra y la velocidad que brinda alcanza para el uso que se va a hacer de

la red del edificio infantil, que se limita a la navegación por internet, la impresión en equipos de la escuela primaria y el intercambio de datos entre dispositivos del mismo edificio, lo cual no influye en esta decisión pues estos equipos están conectados por una LAN cableada. En este caso la tecnología Wi-Fi que se utiliza es el estándar 802.11n, debido a que ofrece una velocidad teórica de hasta 600Mbs y en los equipos actuales es de 300Mbs, lo que supera los 54Mbs ofrecidos por el estándar 802.11g y esto hace que el enlace esté más cerca en velocidad al resto de la red, lo que minimiza el cuello de botella formado en ese punto. Finalmente eligen la opción en donde se integra la antena y el AP. No utilizan ningún simulador de redes para el análisis sino que hacen un estudio del entorno y de las necesidades basándose en la teoría ya existente.

Tercer Ejemplo (Ochoa Correa, 2006)

Trata sobre la ampliación de una LAN mediante dos opciones: la primera usando un punto de acceso para conectar las PC inalámbricas a la LAN y la segunda usando un Router Inalámbrico. Estas dos opciones se observan en la figura 2.3 a y b.



a) **b)**

Figura 2.3. Ampliación de una red LAN a) mediante un punto de acceso, b) mediante un Router inalámbrico.

Este ejemplo tiene un objetivo pedagógico y para el mismo se usa el simulador de redes Packet Tracer. En el caso de la figura 2.3 a) se comprueba la interconexión mediante el comando PING de este simulador y se configuran de forma estática las direcciones IP correspondientes a las PC inalámbricas. Además se plantea que este sistema tiene una

limitante y es que solamente se pueden comunicar entre sí, siempre y cuando los equipos pertenezcan a la misma subred. En la figura 2.3 b) se utiliza un Router Inalámbrico, los equipos que forman parte de la red cableada pertenecen a una dirección de subred diferente a los equipos que pertenecen a la red inalámbrica. Se aprovecha la oportunidad para configurar los equipos de tal forma que las PC pertenecientes a la LAN cableada utilicen direccionamiento IP estático y las PC de la WLAN utilicen direccionamiento IP dinámico, bajo el uso del protocolo DHCP (Protocolo de configuración de host dinámico). También se explica cómo configurar en el simulador Packet Tracer todos los elementos de la red. Este simulador solo permite modelar redes en términos de filtrado y retransmisión de paquetes, por lo que no se puede conocer cuál será el comportamiento de los principales parámetros de la red tales como Delay (Demora), throughput (Razón de transferencia), etc.

2.2 Características de la red

La red que se estudia en este trabajo tiene una dimensión inferior a los 100 metros cuadrados, con un cableado del tipo Fast Ethernet (100Mbps) y debido a nuevas necesidades se requiere que las computadoras inalámbricas se puedan conectar a la red cableada para hacer uso de sus servicios. Se proponen cuatro posibles escenarios, los cuales se representan en el epígrafe 2.5. En la parte superior de la figura 2.4 se muestra una simplificación de la red LAN del Escenario 1. En esta red corren las aplicaciones de internet (HTTP), transferencia de ficheros (FTP) base de datos (database) y correo (e-mail). Teniendo en cuenta todo lo mencionado anteriormente se decidió incrementar el número de usuarios de la red usando una WLAN en modo infraestructura, el estándar elegido fue el IEEE 802.11g, el cual se explica en el sub-epígrafe 1.3.4, podemos destacar que trabaja en la banda de los 2.4GHz y tiene una velocidad de hasta 54Mbps. En la figura 2.4 se puede observar una representación simplificada de los escenarios 2, 3 y 4.

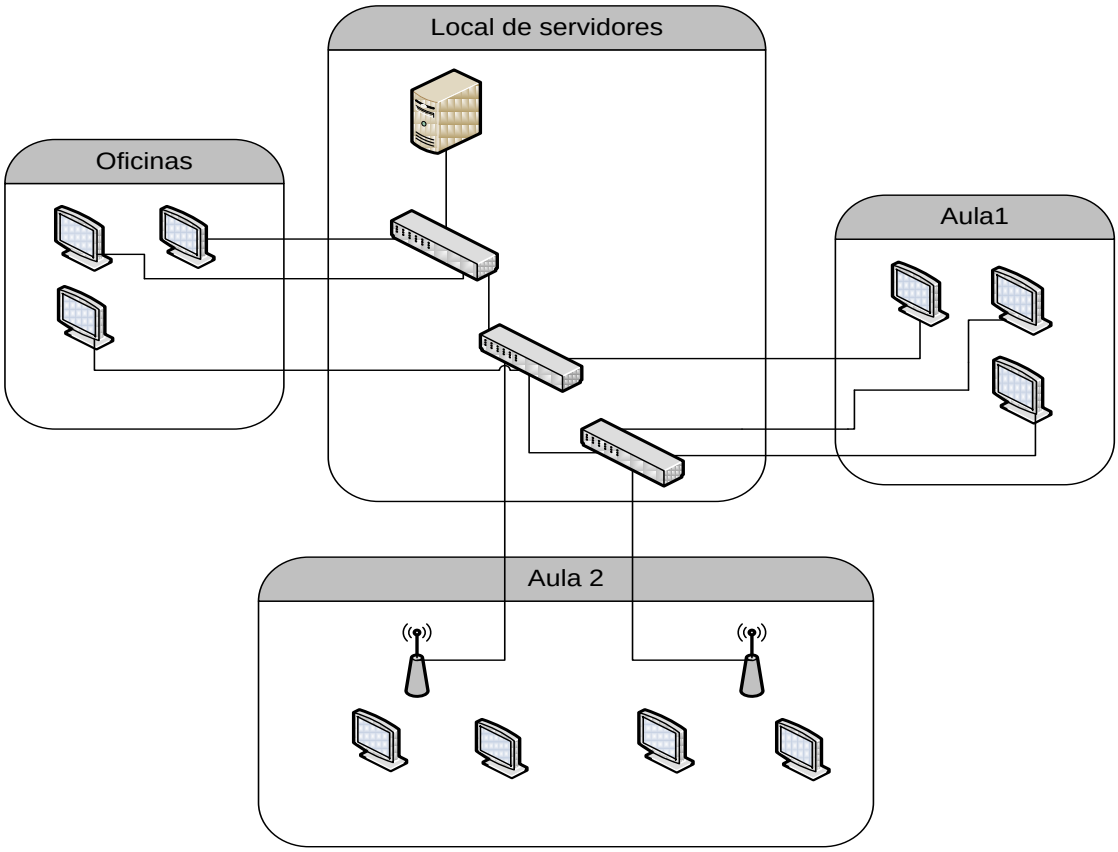


Figura 2.4. Escalabilidad de la red LAN usando WLAN.

2.3 Simuladores de redes

Cada día es más necesario realizar un análisis previo a la ampliación real de cualquier red, para de esta manera conocer cuál será el comportamiento de los principales parámetros de esta y así evitar el posible descontento de los usuarios o un gasto innecesario. Este análisis se puede llevar a cabo con diferentes simuladores de redes, por ejemplo: Omnet++, Network Simulator (NS), COMNET III y OPNET Modeler, entre otros. El objetivo general de estos simuladores es crear un modelo lo más parecido a la realidad, para poder analizar mediante la simulación el posible comportamiento de una red antes de que esta se lleve a la práctica. En este trabajo se decidió utilizar el OPNET Modeler (Optimized Network Engineering Tools), debido a las características y ventajas que este presenta.

2.4 Características y ventajas del OPNET Modeler

Es un lenguaje de programación orientado a la comunicación de datos con varias librerías de modelos de objetos de red, estas permiten acceder a un gran número de aplicaciones y protocolos como: HTTP (Hypertext Transfer Protocol o Protocolo de Transferencia de Hipertexto), TCP (Transmission Control Protocol o Protocolo de Control de Transmisión), Frame Relay (Frame-mode Bearer Service), Ethernet, LANs, 802.11 (Wireless), ect.

Otras ventajas de este simulador de redes son:

- Brinda a las Universidades e ingenieros una forma efectiva de mostrar los diferentes tipos de redes y protocolos.
- Ofrece una amplia visibilidad y control entre dominios de infraestructura.
- Es un software orientado a simular objetos mediante un editor gráfico que permite diseñar una topología de red, soporta un amplio rango de tecnologías tipo LAN, MAN (Metropolitan Area Network o Red de Área metropolitana) y WAN.
- Existe una versión gratis del OPNET que puede ser utilizada en cualquier universidad.
- Permite observar el tráfico por la red a través de una animación, durante y después de la simulación. Los resultados se muestran mediante gráficos estadísticos.

Estas características y ventajas del OPNET Modeler han hecho que este software sea utilizado en las universidades, tanto para el proceso docente como en la realización de análisis previos al montaje de una red real.

2.5 Creación y representación de los Escenarios a simular

Para la creación de estos escenarios lo primero que se hizo fue definir un nuevo proyecto en el OPNET Modeler 14.0, ver Anexo I, en la tabla 2.1 podemos observar los elementos seleccionados en la creación de los escenarios.

Tabla 2.1. Elementos seleccionados en la creación de los escenarios

Pasos	Opción seleccionada
Initial Topology	Create empty scenario
Choose Network Scale	Office
Specify Size	100metros por 100metros
Select Technologies	Ethernet y wireless_lan_adv

Luego se seleccionaron de la paleta de objetos los elementos mostrados en el Anexo II donde se puede destacar que los enlaces cableados son del tipo bidireccional con una velocidad de 100Mbs.

Los escenarios quedaron como se muestran a continuación:

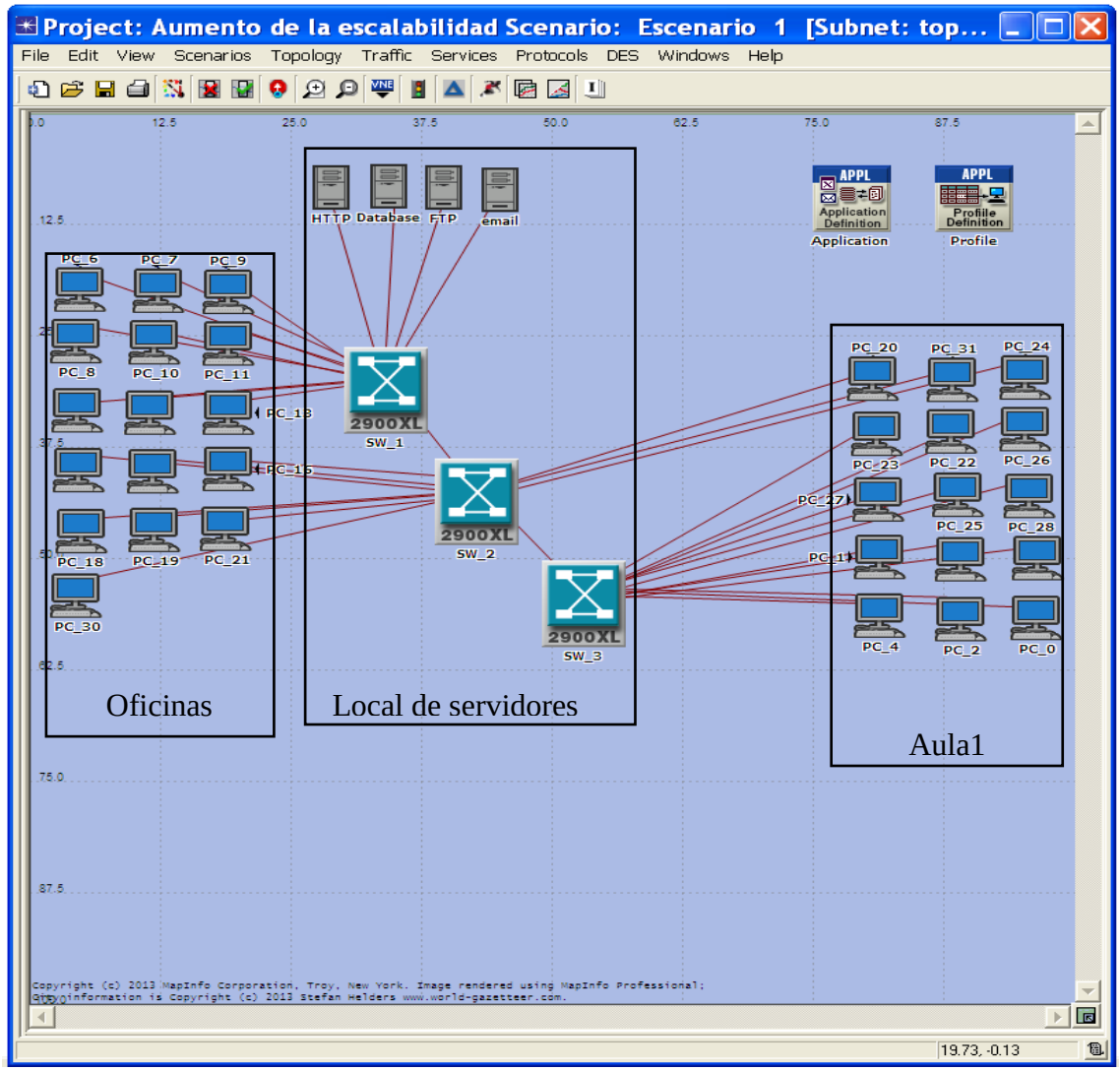


Figura 2.5. Red LAN. Escenario 1.

El escenario 1 (E1) es una representación de una red LAN que cuenta con 31 PC, 3 switch y 4 servidores que brindan servicios de HTTP, FTP, database y e-mail. Partiendo de este escenario otros tres fueron creados, los cuales se describen a continuación.

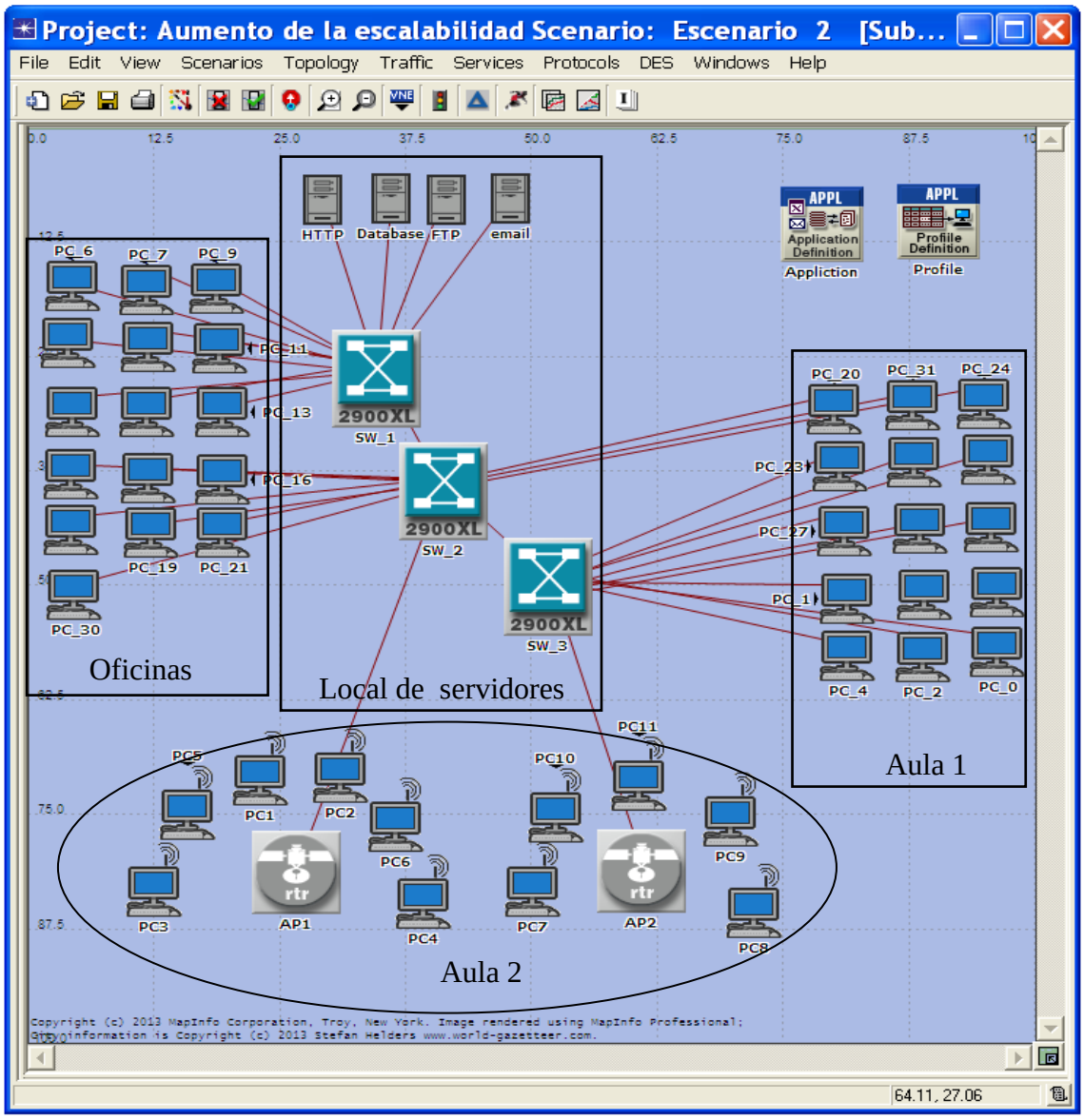


Figura 2.6. Aumento de la escalabilidad usando WLAN. Escenario 2.

El escenario 2 (E2) representa el aumento de la escalabilidad de la red LAN del escenario 1 mediante el uso de 11PC inalámbricas conectadas a 2 AP, por lo que este escenario cuenta con un total de 42 PC e igual número de switch y servidores que el escenario 1.

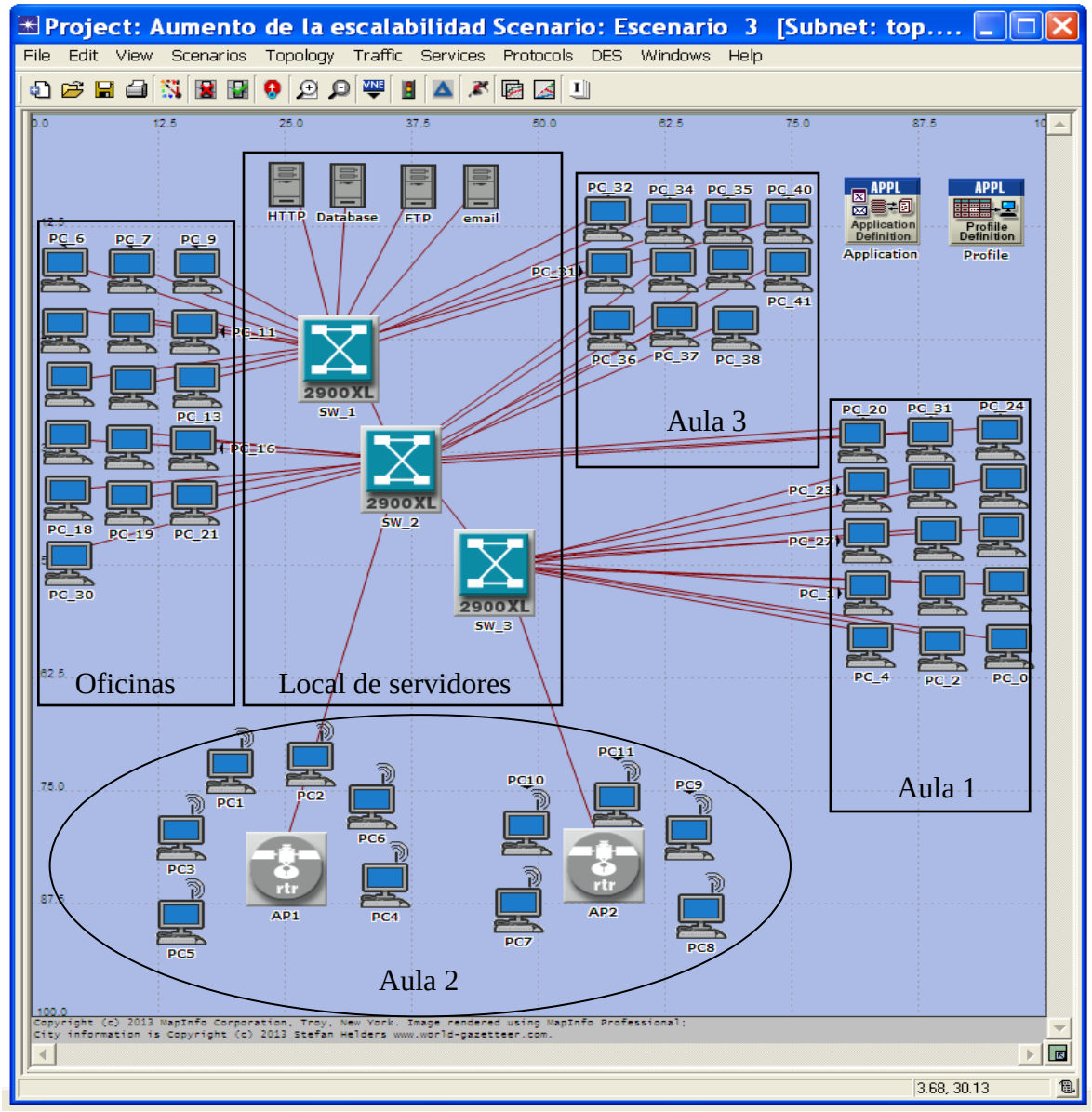


Figura 2.7. Aumento del número de PC cableadas de E2. Escenario 3.

El escenario 3 (E3) es una ampliación de la parte cableada del escenario 2, aumentando 11 PC, por lo que este escenario cuenta con 53 PC en total.

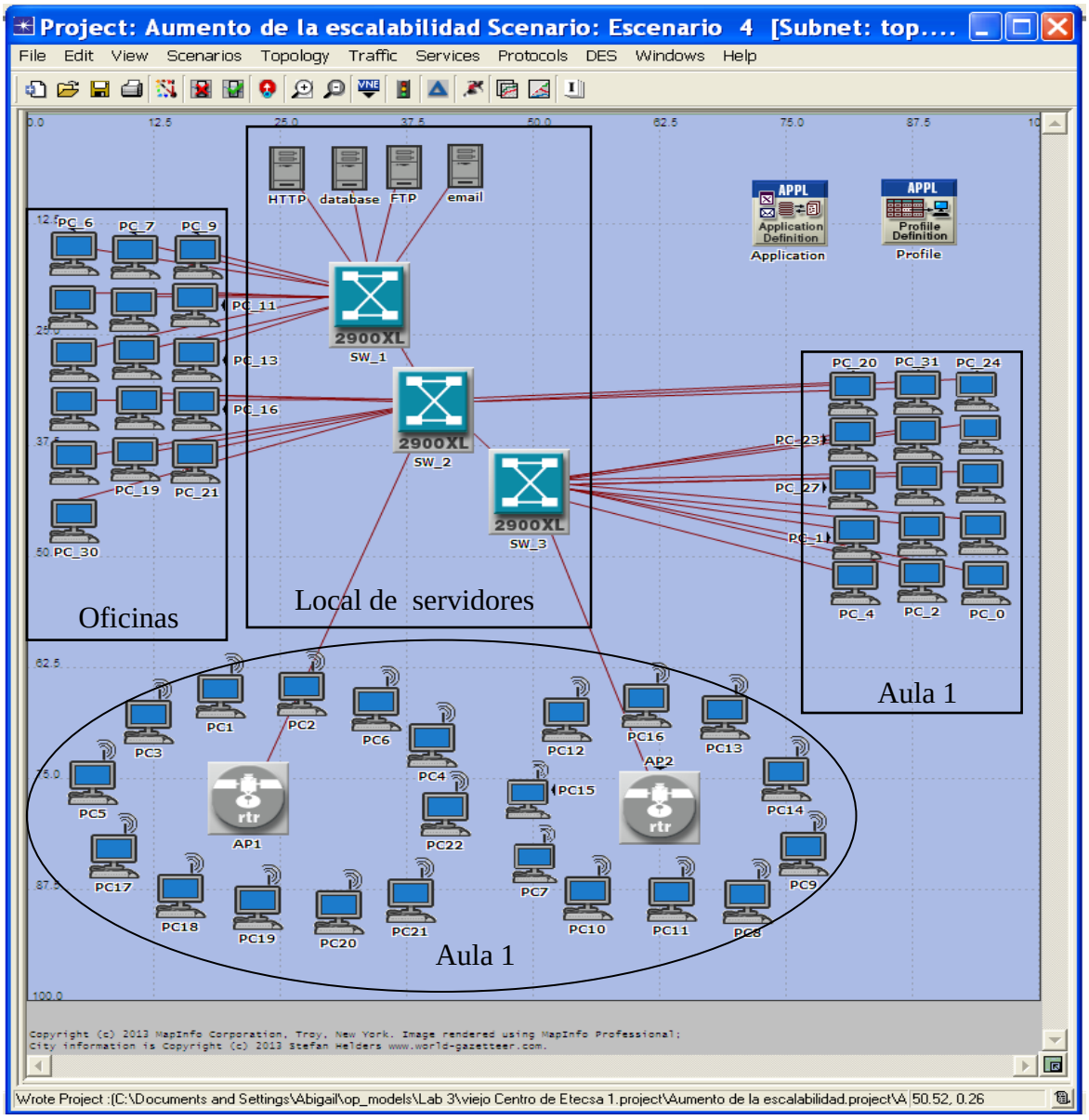


Figura 2.8. Aumento del número de PC inalámbricas de E2. Escenario 4.

En el escenario 4 se han incrementado 11PC inalámbricas al escenario 2, por lo que ahora la WLAN tiene 22PC y la red un total de 53PC

2.6 Configuración de las Aplicaciones y los Perfiles

2.6.1 Configuración de las aplicaciones

Para configurar las aplicaciones se marca clip derecho sobre el elemento **Application Configuration** y se escoge la opción **Edit Attributes**, donde se puede especificar la magnitud y el tipo de tráfico, pero en este caso se marca Default como se puede observar en

la figura 2.9. Las características antes mencionadas se especifican en el elemento Profile Configuration.

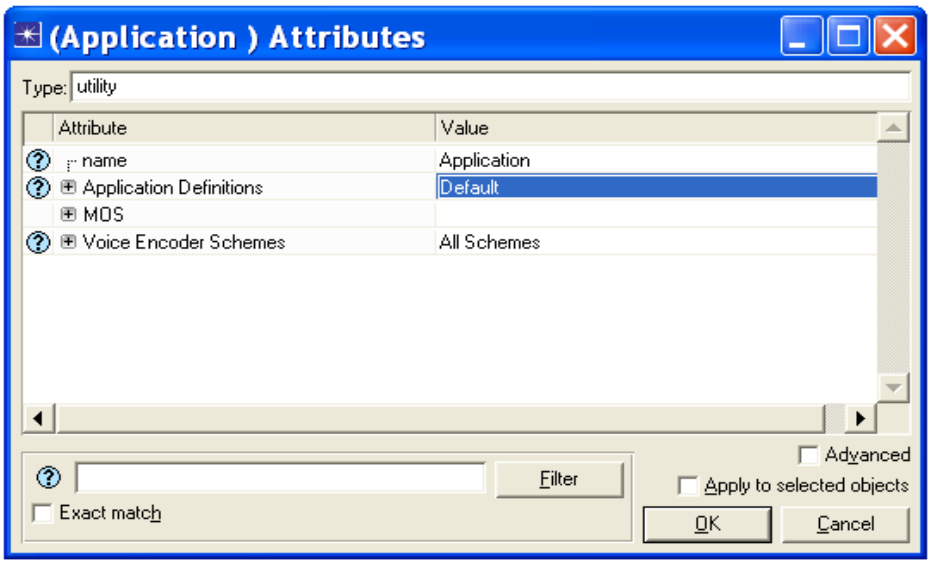


Figura 2.9. Configuración de las aplicaciones.

En la figura anterior además de seleccionar **Default** se cambió el nombre (name) y se puso Application.

2.6.2 Configuración de los perfiles

Se marca clip derecho sobre el elemento **Profile Configuration**, **Edit Attributes** y una vez en esa ventana se realizan todos los pasos mostrados en la figura 2.10.

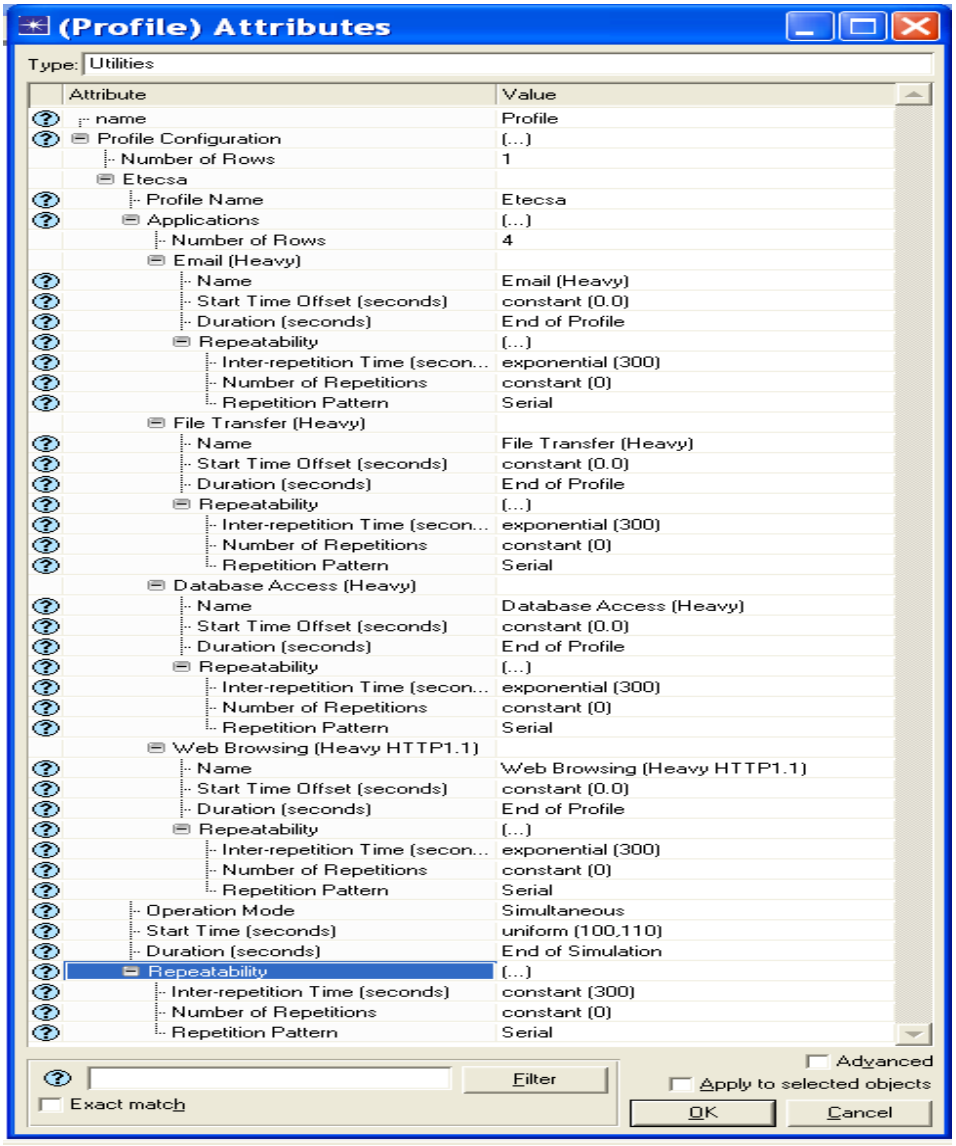


Figura 2.10. Configuración del perfil de aplicaciones.

Para llegar a lo mostrado en la figura 2.10 primero se desplegó **Profile Configuration** y al lado de **Number of Rows** en la tercera fila se pone **1**, debido a que todas las PC reciben todas las aplicaciones configuradas en Profile Configuration, por lo que no hay necesidad de hacer más de un perfil de configuración, el nombre del profile elegido fue **Etecsa**.

Al desplegar Aplicación en **Number of Rows** se pone 4 debido a que serán 4 aplicaciones: internet (HTTP), transferencia de ficheros (FTP), base de datos (database) y correo (e-mail), las que se ponen en Heavy para que el tráfico sea alto en todas y así poder evaluar la red en la peor de las situaciones. Todas estas aplicaciones se eligieron de 16 posibles,

debido a que se editó el elemento **Application Configuration** seleccionando la opción por default, en realidad son 8 aplicaciones con 2 variantes, una con tráfico más suave y la otra más fuerte. Para editar las opciones de Start time Offset, hacer clic en **Edit** al lado de **Start time Offset (seconds)** en cada una de las aplicaciones y se editan los datos tal como se muestra en la figura 2.11.

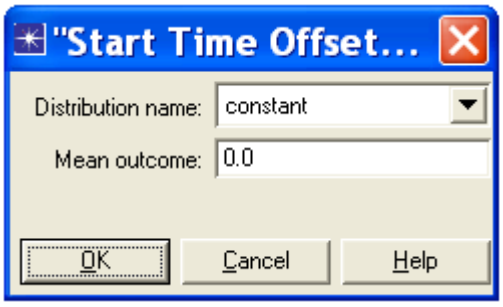


Figura 2.11. Ventana de configuración de Star Time Offset.

Para que aparezca Constant (0) al lado de Number of Repetitions se hace lo mismo que en figura 2.11, pero en Mean outcome solo se puso 0.

En Operation Mode (Modo de operación) se pone simultaneous porque de esta manera el tráfico de cada aplicación será mayor, debido a que todas las PC acceden a la red al mismo tiempo, lo cual permite probar la red en una situación extrema.

De esta manera queda configurado el perfil, o sea el tipo de tráfico ya sea constante u otro tipo de distribución y los parámetros que la definen. Los demás parámetros de la figura 2.10 que no se mencionaron es porque se dejan por defecto.

2.7 Configuración de la LAN

Para la configuración de la LAN se sigue el siguiente orden:

- Configuración del switch.
- Configuración de los servidores.
- Configuración de las computadoras (PC) cableadas.

2.7.1 Configuración del switch

El switch seleccionado es del tipo Cisco catalyst 2924-XL cuyas características se pueden observar en la tabla 2.2.

Tabla 2.2. Características del Switch Cisco catalyst 2924-XL (Álvarez Valderas, 2010)

Características	Cisco catalyst 2924-XL
Cantidad de Puertos	24 x Ethernet 10 Base-T, terminal, Ethernet 100 Base-TX
Velocidad de transferencia de datos	100 Mbps
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Protocolo de gestión remota	SNMP, RMON
Tecnología de conectividad	Cableado
Modo Comunicación	Semidúplex, dúplex pleno
Protocolo de conmutación	Ethernet
Tamaño de tabla de dirección MAC	2 k de entradas
Indicadores de estado	Estado puerto, actividad de enlace, estado de colisión, alimentación
Características	Motorización en red, capacidad dúplex, activable
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.3x

2.7.2 Configuración de los servidores

Para la configuración del servidor de correo (e-mail), se hace clic derecho sobre este y se elige la opción **Edit Attributes**, una vez ahí se da clic izquierdo en la columna de value en la fila de **Application Supported Services,** se selecciona **Edit** y entonces aparece la ventana que se muestra en la figura 2.12, los demás elementos no se modifican.

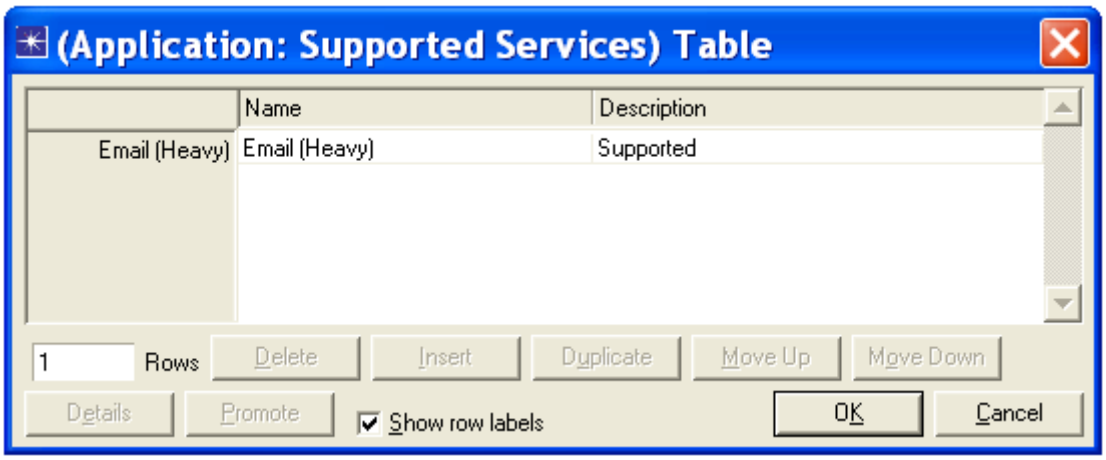


Figura 2.12. Aplicación soportada por el servidor de e-mail.

En figura 2.12 se pone **1** al lado de Rows (filas) porque ese servidor solo brindará un servicio, debajo de name se hace clic izquierdo y se elige **Email (Heavy)** debido a que este será el servicio ofrecido por este servidor.

Los servidores de HTTP, database y FTP se configuran de forma análoga al servidor de email, solo que en la figura 2.12 debajo de name se elige **Web Browsing (Heavy HTTP .1), File Transfer (Heavy), Database Access (Heavy),** respectivamente en cada servidor por separado**.**

2.7.3 Configuración de las PC cableadas

Hacer clic derecho sobre una PC cableada, seleccionar la opción **Select Similar Nodes** para que de esta manera queden seleccionadas todas las PC de ese tipo, luego se hace clic derecho sobre cualquiera de las PC seleccionadas y se va a **Edit Attributes** y se realiza todo lo que se ve en figura 2.13.

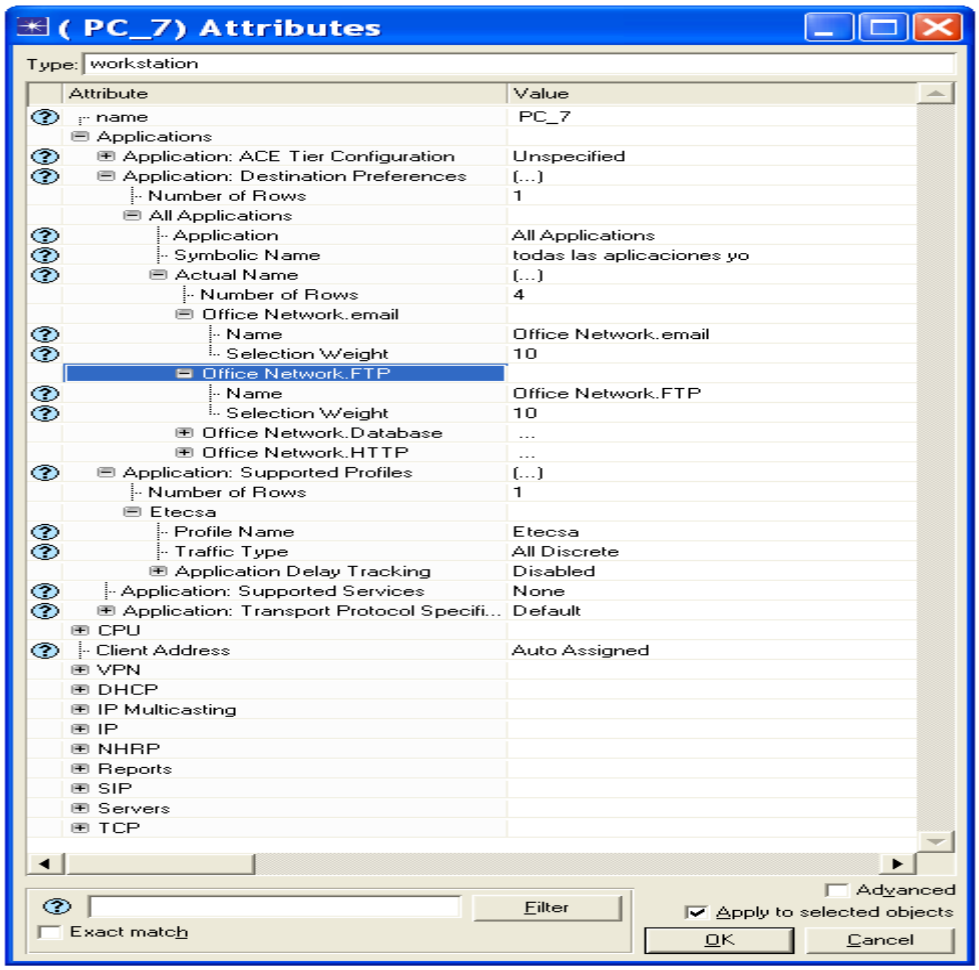


Figura 2.13. Configuración de las PC cableadas.

Para llegar a lo mostrado en la figura 2.13, primero se despliega **Application** y **Application: Destination Preferences**. Justo debajo de este, al lado de Number of Row (número de filas) se puso **1** y al lado de Application se dejó **ALL Application** (todas las aplicaciones), debido a que no se le dará preferencia a ninguna aplicación. Se puso en Name symbolic (nombre simbólico) **Todas las aplicaciones yo.** Debajo de Actual Name en Number of Row se pone 4, debido a que estas serán la cantidad de aplicaciones que se configurarán. Se despliega la primera de las cuatro filas con esta opción que aparece debajo de Actual Name y al lado de Name se selecciona **Office Network.email.** Se hace lo mismo en las otras tres filas con la diferencia de que al lado de Name se selecciona **Office Network.FTP, Office Network.Database** y **Office Network.HTTP** respectivamente. Esto se hace porque email, FTP, Database y HTTP son los nombres de los 4 servidores que atienden estas aplicaciones. Luego se despliega **Application Supported Profiles,** se pone **1**

al lado de Number of Row y se selecciona Etecsa al lado de Profile Name, quedando así todas las PC cableadas con el perfil definido en Profile Configuration (Configuración del Perfil). Luego de realizar todos los pasos mencionados, marco el recuadro de al lado de Apply to selected objects (aplique a los objetos seleccionados), con esto se garantiza que todas las PC seleccionadas al principio queden con la misma configuración. Para salir de la ventana marco OK, quedando de esta manera configuradas las PC cableadas.

2.8 Configuración de la WLAN

En este epígrafe se configuran los equipos inalámbricos, primero las PC y luego los AP.

2.8.1 Configuración de las PC inalámbrica

En el escenario 3 para configurar las computadoras (PC) inalámbricas, se deja apretada la tecla control y se van marcando todas estas PC, luego se da clip derecho sobre una de ellas, se selecciona la opción **Edit Attributes** y se marca al lado Apply to selected objets para que todas estas PC marcadas queden igualmente configuradas. En la ventana de **Attributes** la configuración de **Application Destination Preference** y de **Application Supported Profiles** se realiza igual que en la figura 2.13 donde se ve la configuración de las PC cableadas, en el caso de las PC inalámbricas tienen en esta ventana una fila llamada **Wireless LAN**, que también hay que configurar y se hizo como se muestra en figura 2.14.

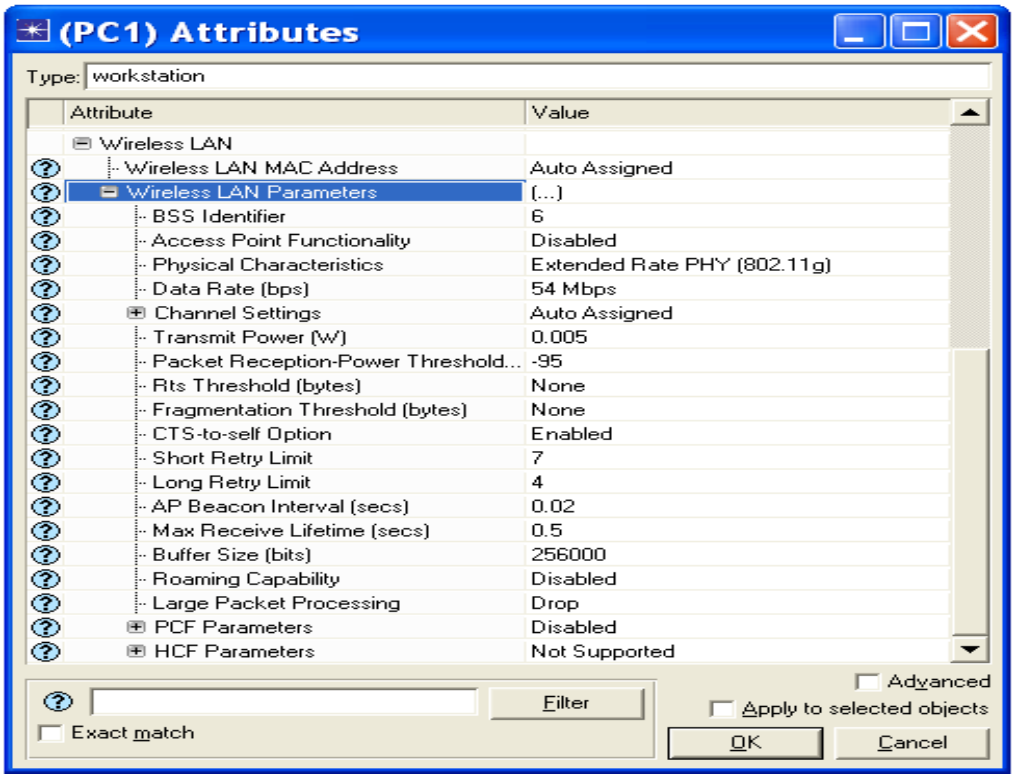


Figura 2.14. Configuración de los parámetros WLAN de las PC inalámbricas conectadas al AP 1.

En BSS identifier (identificador de conjunto de servicio básico) se pone 6, este número tiene que coincidir con el del AP 1 en esa opción, para que estas PC puedan conectarse a ese AP, debido a que en el modo infraestructura el BSS identifier corresponde al punto de acceso de la dirección MAC. Al lado de **Physical Characteristic (**Características físicas) se elige **Extended Rate PHY (802.11g)** debido a que el estándar elegido para este trabajo fue el 802.11g. En **Data Rate (bps)** (Razón de datos en bit/seg) se selecciona 54Mbps debido a que esta es la máxima velocidad que ofrece el estándar seleccionado. Los demás parámetros se dejaron por defecto. Las PC que se comunican a través del AP 2 se configuran de igual forma, solo que en **BSS Identifier** se pone 5 y este número se hace coincidir **con el puesto en BSS Identifier** en el AP 2. Las PC inalámbricas del escenario 4 se configuran de forma análoga a las del escenario 3, solo varía el número puesto en **BSS Identifier** ya que se aumentó a 12 y 10 las PC correspondientes a los AP 1 y 2 respectivamente.

2.8.2 Configuración de los AP

Para la configuración del AP 1 del escenario 3 se marca este y se selecciona la opción Edit Attributes y entonces aparece la figura que se muestra a continuación:

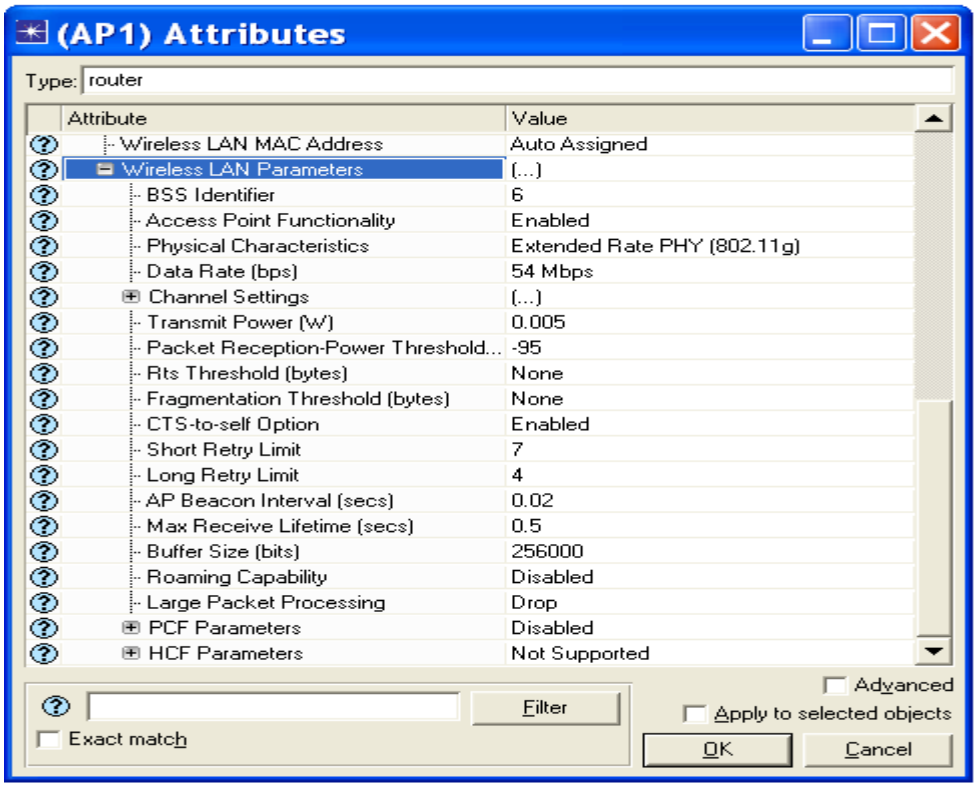


Figura 2.15. Configuración de los parámetros WLAN de AP 1.

Se puede observar que se realizan las mismas modificaciones realizadas en figura 2.14 y además se habilita la opción **Access Point Functionality** (función de punto de acceso) seleccionando Enabled al lado de esta, los demás parámetros se dejan por defecto. El AP 2 del escenario 3 se configura de forma análoga al AP 1.

2.9 Selección de las Estadísticas que se valorarán

Luego de tener los escenarios y haber configurado todos los elementos de estos, se debe realizar una selección de las estadísticas a analizar para valorar el comportamiento de una red LAN a la que se le realizó un incremento de la cantidad de usuarios mediante el uso de WLAN. Para esto se marca clip derecho en el espacio de trabajo vacío si se desea medir estadísticas de la red completa o sobre algún nodo o enlace para medir el comportamiento

de una parte específica de la red. Luego de cualquiera de las 2 opciones mencionadas se elige **Choose Individual DES Statistics** y una vez ahí se marcan las estadísticas tal como se muestra en la figura 2.16.

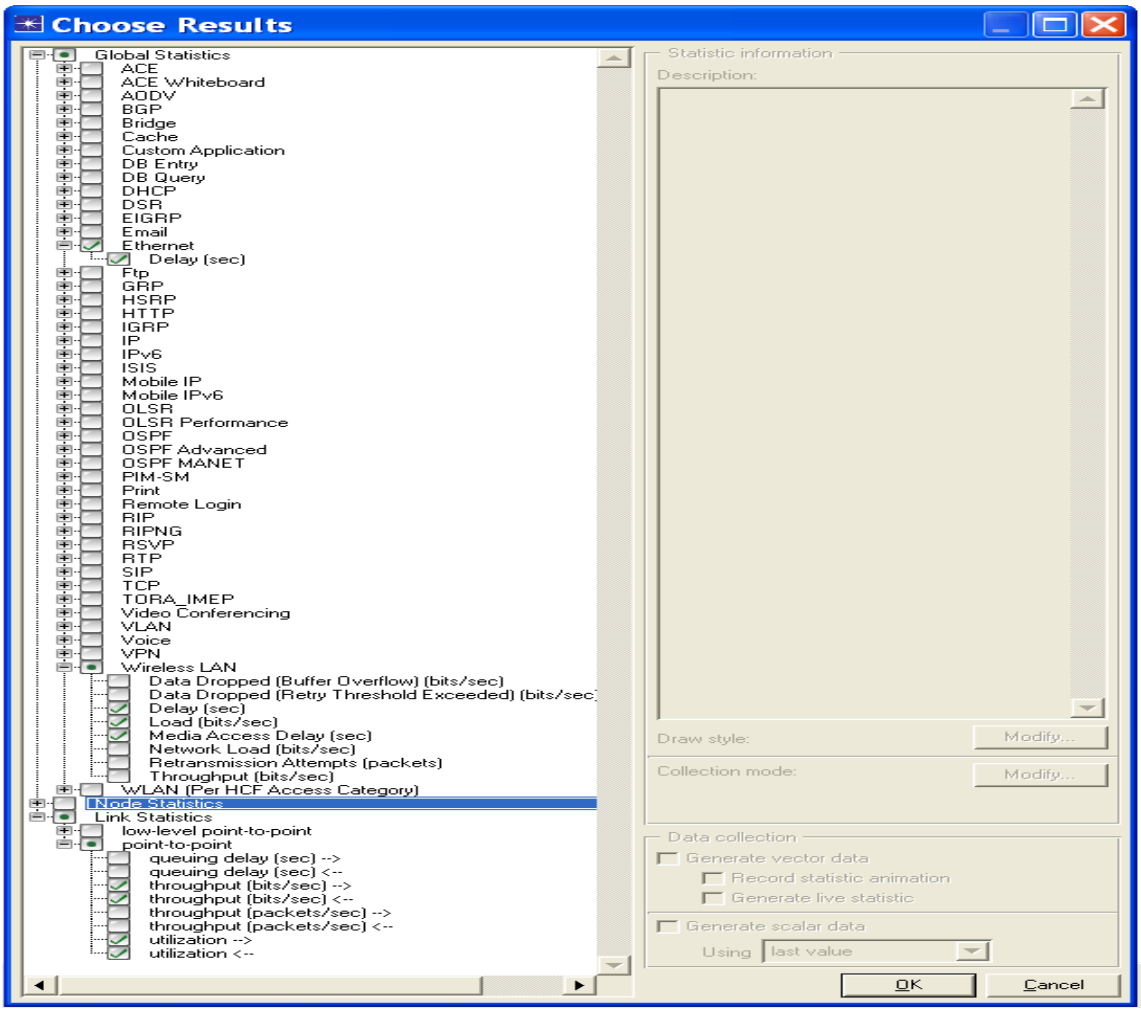


Figura 2.16. Parámetros que se medirán.

En la figura 2.16 se pueden ver parte de las estadísticas seleccionadas en los cuatro escenarios, como es lógico en el escenario 1 no está presente lo relacionado con WLAN pues este no cuenta con parte inalámbrica. Se seleccionaron varios parámetros que normalmente se valoran en las redes LAN y otros que se miden en las WLAN, con el objetivo de tener una idea completa del comportamiento de la red luego de la ampliación. Esta selección estuvo basada fundamentalmente en el estudio de los siguientes documentos: (Álvarez Paliza, 2013, Kumar Jha, 2010, Soungalo and Renfa, 2010, Khosa et al., 2010).

2.10 Conclusiones parciales

Se dispone en este momento en el simulador de redes OPNET Modeler de la configuración de diferentes escenarios donde se incrementa de la cantidad de usuarios de una red LAN usando WLAN. En esta configuración están las principales características de los escenarios como: el número de PC cableadas e inalámbricas y demás equipos de la red, las aplicaciones que corren en esta, el tipo de cableado, el estándar usado en la WLAN, entre otros elementos. Lo anterior es lo que permite la realización de las simulaciones y la obtención de los gráficos que hacen posible el análisis de parámetros como la demora, la razón de transferencia y la carga.

CAPÍTULO 3. ANÁLISIS DEL COMPORTAMIENTO DE LOS PARÁMETROS DE LA RED

En este capítulo se realiza una valoración del comportamiento de la red en los diferentes escenarios de expansión propuestos. Para esto se analizan los principales parámetros de la red tales como la carga (load), los diferentes tipos de demora (delay), la razón de transferencia (througput) y la utilización del canal. Este análisis se basa en los gráficos obtenidos en el simulador de redes OPNET Modeler.

3.1 Análisis de la carga (load)

La carga es el total de bits/segundos recibidos de los niveles superiores en todos los nodos de la red. En este epígrafe se analiza la carga a la que están sometidos los servidores, para saber si estos pueden soportar las nuevas PC instaladas.

Primero se comprueba si los servidores del escenario 1 no están al tope de su capacidad mediante la siguiente figura:

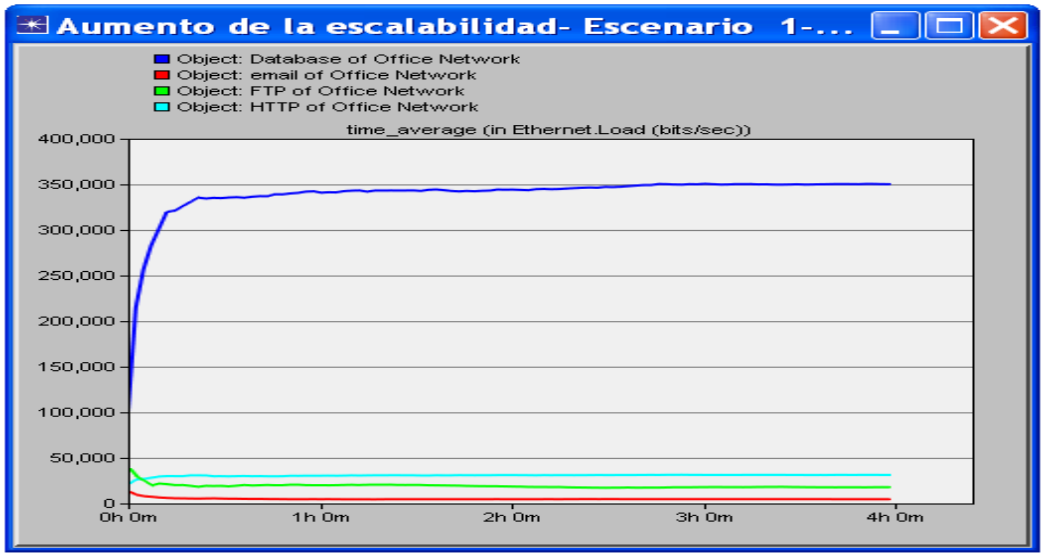


Figura 3.1. Carga en bits/seg de los servidores del primer escenario.

Se puede observar en la figura 3.1 que el servidor que soporta la mayor carga es el de base de datos (database), pero esta es de solo 350000bits/seg (0.35Mbps) y la carga máxima que puede soportar este servidor es de 100Mbps, esto indica un buen uso del servidor, por lo que puede soportar un mayor número de PC.

Teniendo en cuenta que las PC usadas para el aumento de la escalabilidad en los escenarios 2, 3 y 4 incluyen las 4 aplicaciones configuradas de igual manera que en el escenario 1, es de esperar que el servidor con mayor carga continúe siendo el de base de datos por lo que se analiza este por separado. (Ver figura 3.2).

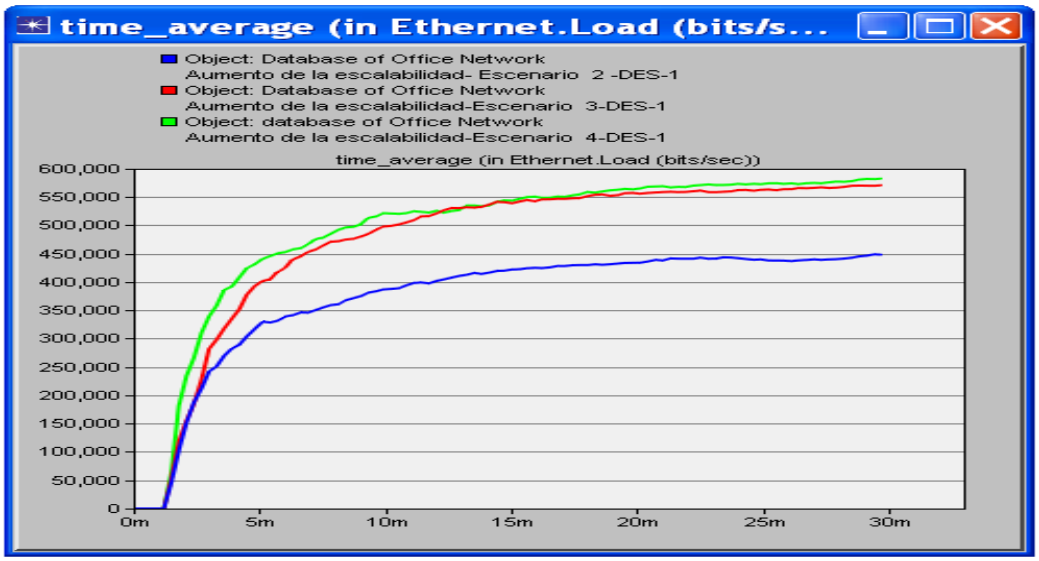


Figura 3.2. Carga en bits/seg del servidor de base de datos en los escenarios 2, 3 y 4.

Se puede observar que en los escenarios 3 y 4 que son los de mayor carga, esta es de aproximadamente 550000bits/seg (0.55Mbps) y esto ni siquiera se acerca a los 100Mbps, por lo que se puede decir que este servidor está en capacidad de soportar sin problemas las ampliaciones realizadas.

Otro lugar importante donde se debe medir la carga es en los puntos de acceso (AP), debido a que este es el que gestiona todo el tráfico recibido y enviado por las PC inalámbricas que se encuentran en su área de cobertura.

Se analiza solo el AP1 debido a que en ningún escenario el AP2 tiene más PC inalámbricas que el uno, por tanto basta con garantizar el buen funcionamiento de este.

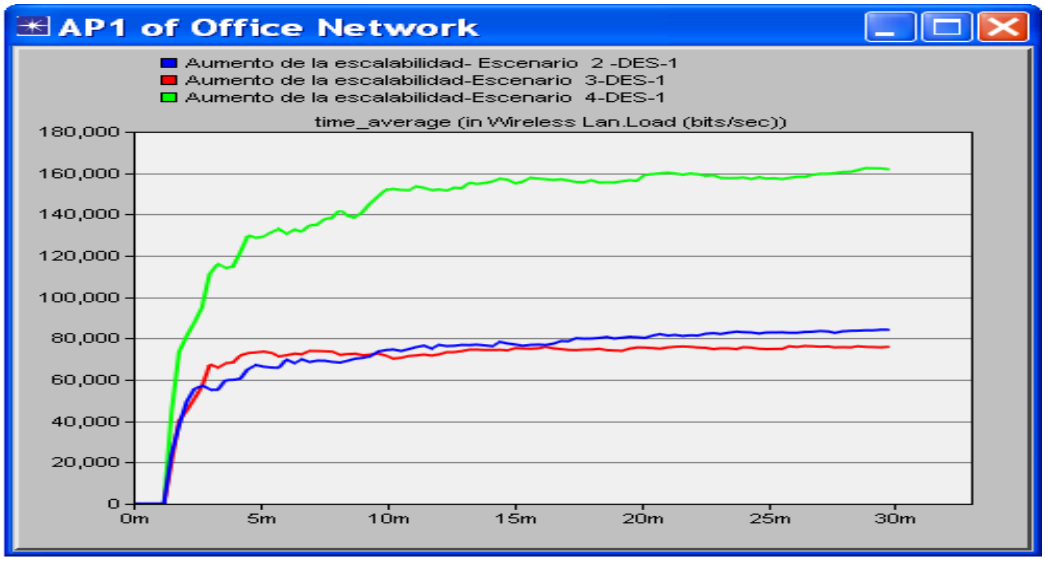


Figura 3.3. Carga en bits/seg del AP 1 en los escenario 2, 3 y 4.

Se puede observar en la figura 3.3 que en el escenario 4 se duplica la carga en el AP 1, debido a que cuenta con el doble de las PC inalámbricas que tiene en los escenarios 2 y 3, pero el valor de la carga es de solo 160000bit/seg (0.16Mbps), lo cual no representa un problema porque el estándar usado es el 802.11g el cual permite velocidades de hasta 54Mbps.

3.2 Análisis de los diferentes tipos Demora (Delay) en la red

En este epígrafe se analiza el comportamiento de la demora Ethernet (Ethernet delay), la demora en la WLAN y la demora media de acceso, con el objetivo de conocer si se producen o no afectaciones producto del aumento de la escalabilidad en los diferentes escenarios.

3.2.1 Demora Ethernet (Ethernet delay)

Esta estadística representa la demora extremo a extremo de todos los paquetes recibidos por todas las estaciones. En la siguiente figura se analiza este parámetro en el escenario 1.

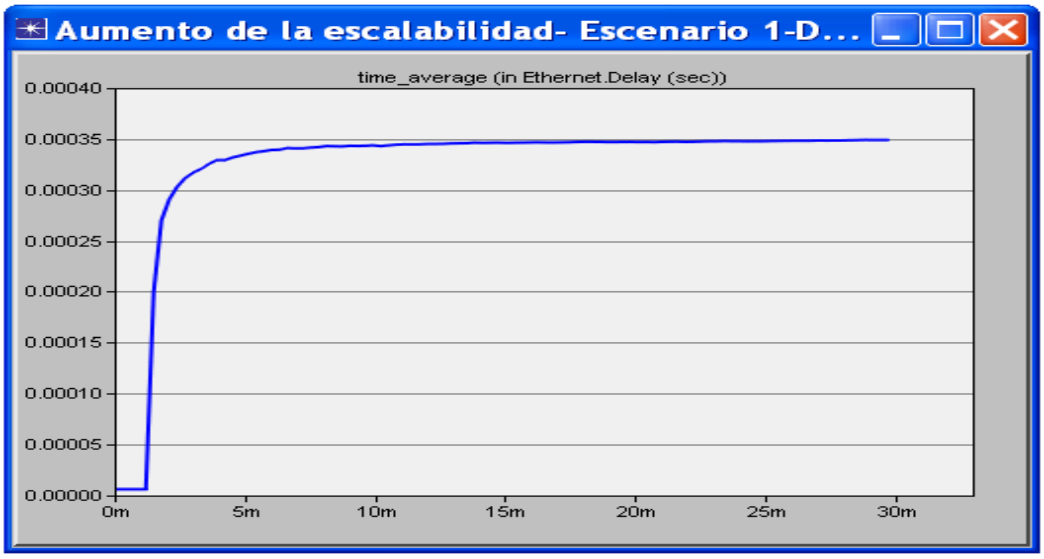


Figura 3.4. Demora Ethernet en el escenario 1.

En la figura 3.4 se observa que la demora aumenta bruscamente en los primeros minutos y luego se estabiliza en 0.35 milisegundos (ms), lo cual indica que no hay congestión en la red porque de existir esta demora tendería a infinito.

Ahora se comprueba si con el aumento de la escalabilidad en los diferentes escenarios la demora Ethernet sufre alguna variación que pueda afectar el servicio.

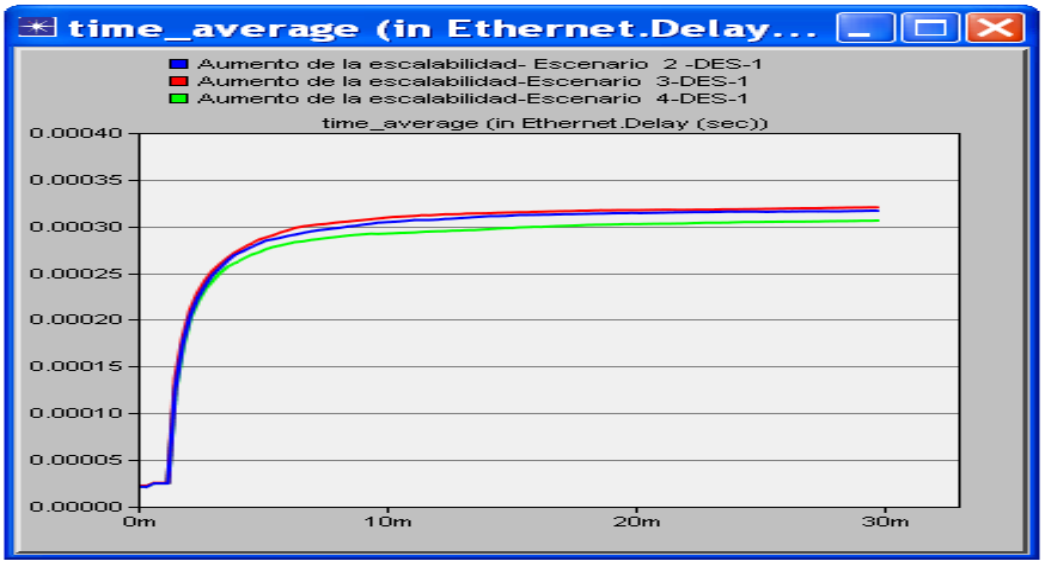


Figura 3.5. Demora Ethernet en los escenarios 2, 3 y 4.

Se puede observar en la figura anterior que la demora Ethernet no supera en ningún momento los 0.35ms, que fue el valor de esta en el primer escenario, por lo que queda

demostrado que la demora Ethernet no se ve afectada por las diferentes ampliaciones de la red.

3.2.2 Demora media de acceso (Media Acces Delay)

Este parámetro es el Tiempo total en segundos en que el paquete está en la cola del nivel superior. En la figura 3.6 se puede apreciar el comportamiento del mismo en los escenarios 2, 3 y 4.

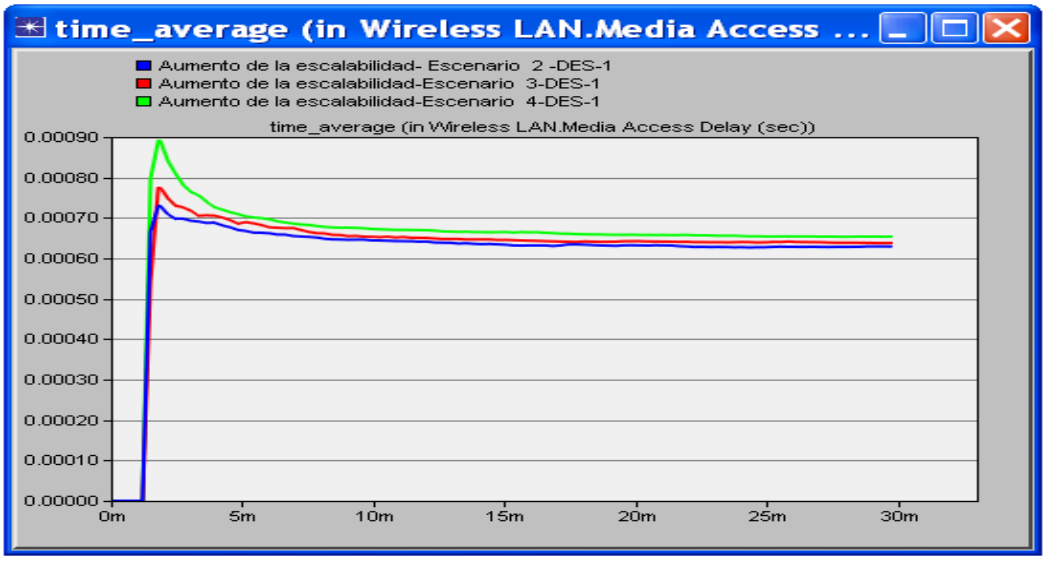


Figura 3.6. Demora media de acceso en la WLAN, escenario 2, 3 y 4.

En la figura anterior se puede observar que en el escenario 4 la demora media de acceso solo sufre un pequeño incremento de aproximadamente 0.025ms, el cual es insignificante si se tiene en cuenta que en este escenario se duplicaron las PC inalámbricas existentes en el escenario 2 y 3.

3.2.3 Demora en la WLAN (Wireless LAN delay)

Este parámetro representa la demora extremo a extremo de todos los paquetes recibidos a nivel MAC en todos los nodos en la red WLAN. Este retardo incluye la demora para acceder al medio, la recepción de todos los fragmentos individuales y las transferencias de las tramas a través del AP si su funcionamiento estaba habilitado.

En la siguiente figura se compara el parámetro anteriormente descrito para el caso de los escenarios 2, 3 y 4:

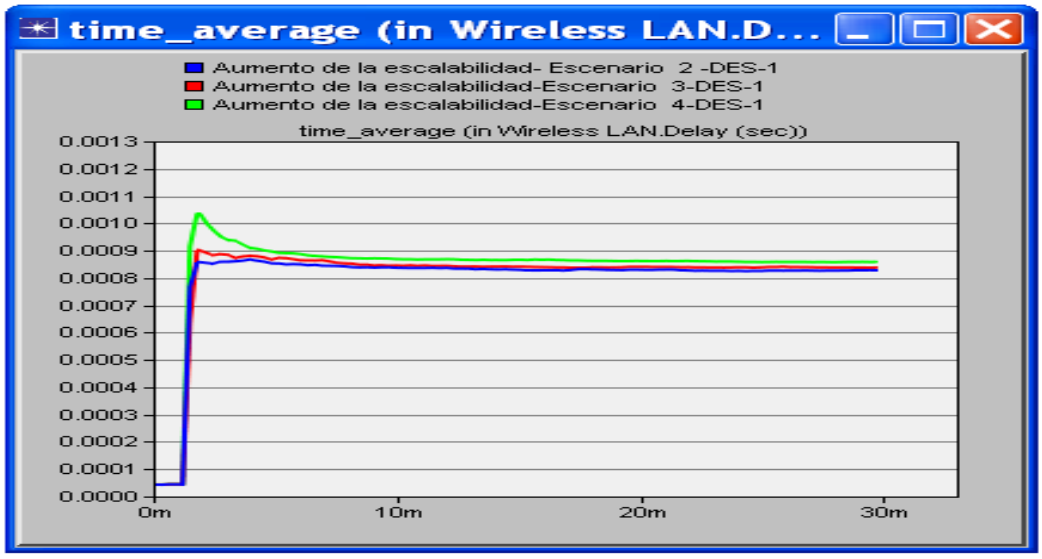


Figura 3.7. Demora en la WLAN, escenarios 2, 3 y 4.

Se puede observar que la diferencia entre la demora en la WLAN del escenario 4 y la del escenario 2 es de aproximadamente 0.025ms, algo insignificante si se tiene en cuenta que se duplicaron las PC inalámbricas. Además este valor indica que de todos los elementos que se incluyen en el cálculo de la demora en la WLAN el único que tuvo una variación perceptible con el aumento de la escalabilidad del escenario 2 fue la demora media de acceso.

3.2.4 Comparación de la demora Ethernet con la demora en la WLAN

En la figura 3.8 se compara la demora Ethernet con la demora en la WLAN, esto se hace solo en un escenario debido a que como ya se observó, estos parámetros no variaron significativamente con los diferentes escenario y el hecho de que en la figura estén solo dos curvas en lugar de ocho brinda una mayor claridad.

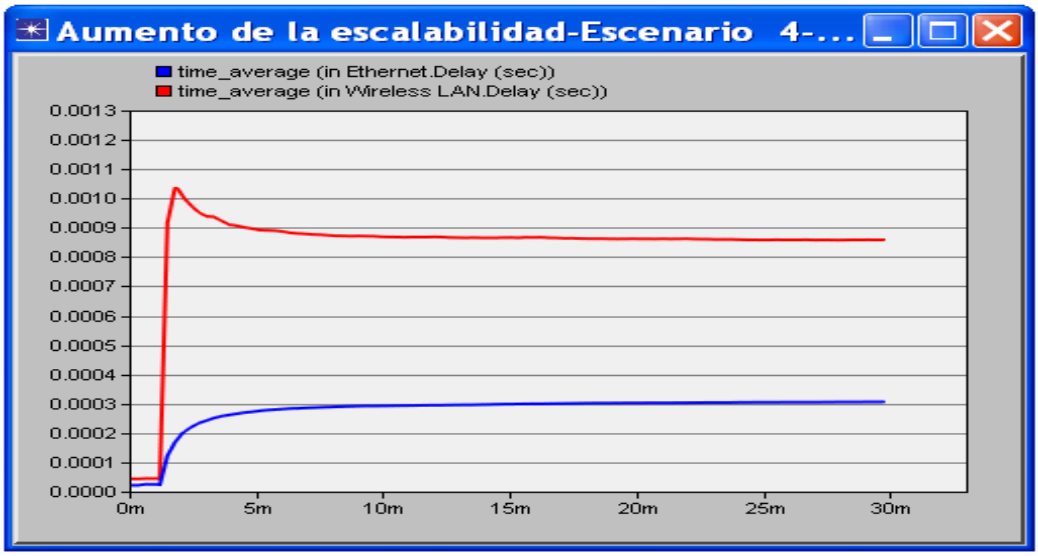


Figura 3.8. Demora etherner contra demora en la WLAN ambas en escenario 4.

Se puede apreciar que la demora en la WLAN casi triplica la demora Ethernet y esto se debe a que las PC inalámbricas requieren de un tiempo extra para acceder al medio.

Esta mayor demora en las redes WLAN demuestra la necesidad de realizar un análisis más fuerte a la hora de aumentar el número de PC inalámbricas o de implementar determinada aplicación en estas.

3.3 Razón de transferencia (througput) y utilización del canal

En este epígrafe se observa el comportamiento del througput y de la utilización del canal con el objetivo de entender porqué a pesar de aumentar la carga con la ampliación de la red, la demora Ethernet y la demora en la WLAN se mantuvieron sin variaciones significativas.

3.3.1 Razón de transferencia (througput)

Este parámetro representa el tráfico total en bits/s recibido de manera exitosa y reenviado a la capa superior. El mismo no incluye las tramas de datos unicast direccionadas de otra MAC, duplicidad de tramas antes de ser recibidas o tramas incompletas.

En la siguiente figura se muestra el comportamiento del througput en la WLAN.

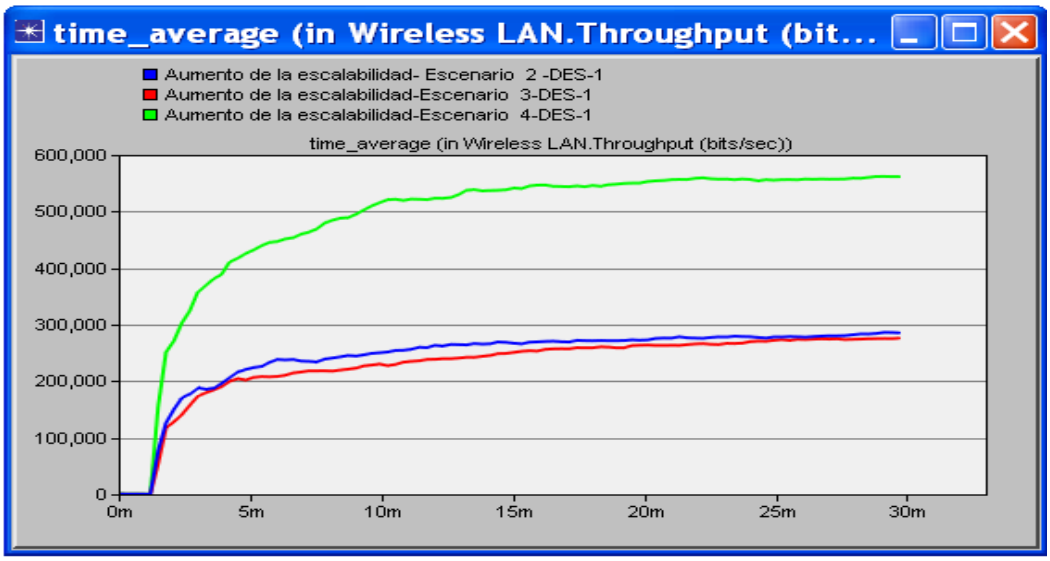


Figura 3.9. Througput en la WLAN, escenarios 2, 3 y 4.

Se puede observar que en el escenario 4, donde se duplican el número de PC inalámbricas de los escenarios 2 y 3, también se duplica la razón de transferencia, lo cual permite que a pesar del aumento del tráfico en bits/segundos se mantenga estable la demora en la WLAN.

Para comprobar este comportamiento del througput también se analiza el enlace entre SW_1 y SW_2, debido a que por su ubicación puede ser una de las conexiones donde se necesite una mayor razón de transferencia. Esta comparación se hizo solamente con el througput enviado de SW_1 a SW_2, para tener solamente cuatro curvas en el gráfico y lograr mayor claridad. Además se comprobó que para este enlace en todos los escenarios el enviado en esa dirección fue ligeramente superior al recibido.

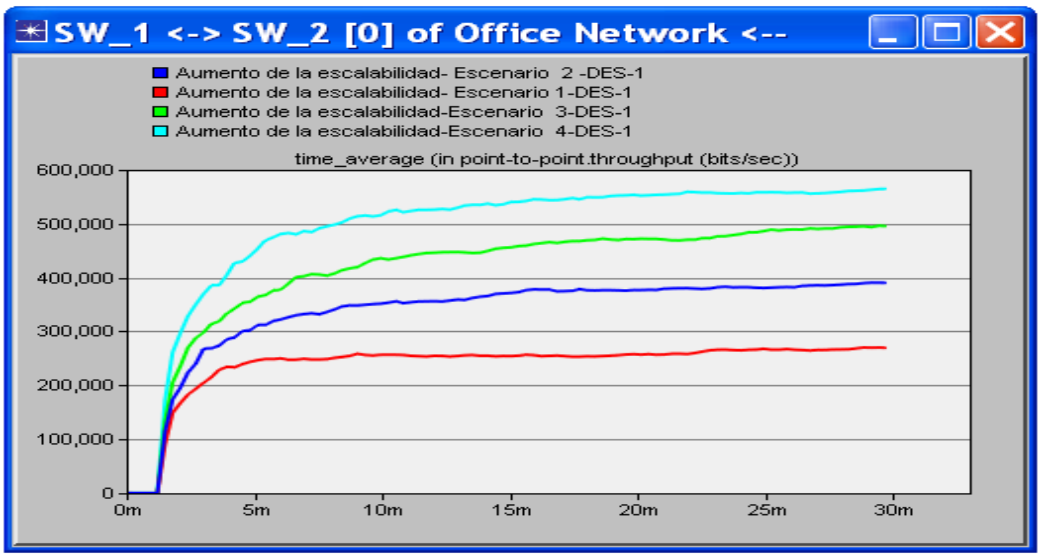


Figura 3.10. Througput en el enlace de SW_2 a SW_1.

Se puede observar que a medida que aumenta el número de PC que tienen que utilizar este enlace para comunicarse con los servidores, aumenta proporcionalmente la razón de transferencia del enlace. Este comportamiento de los enlaces es el que permite que la demora Ethernet se mantenga estable en los diferentes escenarios.

3.3.2 Utilización del canal

Este parámetro indica el porcentaje de utilización del canal y se utiliza para evaluar el grado de uso del ancho de banda. En la siguiente figura se puede ver el comportamiento del mismo en la conexión de SW_1 con SW_2 en el escenario 1 y en el 4.

a) b)

Figura 3.11. Utilización del canal en el enlace SW_1 a SW_2 a) escenario 1 b) escenario 4.

Se puede observar que en el escenario 1 la utilización del canal es muy baja y que en el escenario 4 este aumento no es significativo. Esto indica que hay una gran cantidad de ancho de banda disponible, lo cual permite que al realizar el aumento de la escalabilidad pueda aumentar sin problemas la razón de transferencia y no exista un aumento de la demora Ethernet.

La utilización del canal también se analizó en el AP1 y AP2 de los escenarios 2, 3 y 4, dando un resultado bastante similar a los mostrados en la figura 3.11b. Esto muestra porqué en el escenario 4 en donde se duplicaron las PC inalámbricas la WLAN estuvo en capacidad de duplicar la razón de transferencia y por tanto de lograr que no se produjera una variación significativa en la demora.

Luego de analizar la utilización del canal es evidente que solo se produciría congestión en la red si se realizara un aumento muy grande del número de PC o del tráfico. Teniendo en cuenta todo lo mencionado anteriormente se decidió no seguir ampliando la red, debido a que nuevos escenarios con más PC se analizarían de forma análoga a los ya mostrados.

3.4 Conclusiones parciales

Para el caso de los cuatro escenarios estudiados se comprobó que el comportamiento de la red luego de incrementar la cantidad de usuarios usando WLAN no sufrió modificaciones que afectaran su funcionamiento. Además el estudio realizado en este capítulo puede servir de base para conocer el comportamiento de otras redes y de sus ampliaciones, debido a que se explicaron los significados de diferentes parámetros que se pueden medir utilizando el OPNET Modeler, se mencionaron lugares fundamentales de las redes en donde se debe analizar el comportamiento de cada parámetro y se mostró como llegar a conclusiones mediante el análisis de los gráficos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Como resultado del presente trabajo se arribaron a las siguientes conclusiones:

- Se decidió utilizar el estándar IEEE 802.11g, debido a que el rango y la velocidad que este ofrece son suficientes paras las dimensiones de la red WLAN que se implementó y para las aplicaciones que corren en esta. Además es compatible con el estándar IEEE 802.11b.
- Se definieron: Seguridad, atenuación por obstáculos, Roaming y la asignación de canales, como los principales elementos a tener en cuenta en la implementación de una WLAN.
- Se determinó que para incrementar la cantidad de usuarios de una red LAN usando WLAN se debe utilizar esta en modo infraestructura, debido a que en este las PC inalámbricas pueden integrarse a la red cableada y hacer uso de sus servicios. Teniendo en cuenta lo mencionado anteriormente en los escenarios de expansión propuestos se utiliza este modo de operación.
- Se demostró la potencia de la herramienta de simulación de redes OPNET Modeler, pues permite configurar detalles de la red como por ejemplo el tipo de cableado, el estándar que usa la WLAN, las aplicaciones que corren en la red, la fragmentación o no de las tramas MAC de las PC inalámbricas o de los AP, entre otros elementos. Además permite medir parámetros fundamentales para analizar el desempeño de la red como son la demora, la razón de transferencia y la carga.
- Se comprobó que la demora no necesariamente se ve afectada por el aumento de la cantidad de usuarios o de la carga en los servidores, debido a que se demostró que cuando hay suficiente ancho de banda disponible la red puede aumentar la razón de transferencia y por consiguiente no afectar la demora.

- Se comprobó que la demora en la WLAN es mayor que la demora Ethernet, debido a que las PC inalámbricas requieren un tiempo extra para acceder al medio.
- Se demostró que los diferentes escenarios de expansión estudiados no sufrieron modificaciones que afectaran su funcionamiento. Además se determinó que el análisis realizado puede servir de base en el estudio de redes con mayor complejidad.

Recomendaciones

- Utilizar este trabajo como base para el análisis del incremento de la cantidad de usuarios de una red LAN usando WLAN tanto para valorar el comportamiento de los principales parámetros de la red como para seleccionar la versión del estándar IEEE 802.11 que se debe usar.
- Profundizar en el estudio de los estándares sobre todo del IEEE 802.11ac.
- Se recomienda realizar cambios en los escenarios estudiados que permitan un funcionamiento óptimo de la red.

REFERENCIAS BIBLIOGRÁFICAS

ACERO PALACIOS, R. V. 2007. *Diseño e implementación de una Red LAN y WLAN para brindar servicios y capacidad VPN para la Emñpresa INGELSI CIA.LTDA.* Escuela Politécnica del Ejército. .

AEROHIVE, N. 2013. Guía del Comprador de WLAN Available: http://aerohive.com/pdfs/international/Aerohive-WLAN-Eval-Guide-2012-2013_Spanish.pdf.

AHMAD, A. 2005. *Wireless and mobile data networks*, Wiley-Interscience.

ÁLVAREZ PALIZA, F. 2010. Redes de Área Local Inalámbricas (WLAN). Available: 10.12.1.64/docs/FIE/Asignaturas/Telecomunicaciones y Electrónica/Redes I/Notas del Profesor/Tema 4.

ÁLVAREZ PALIZA, F. 2013. Redes Inalámbricas de Área Local (WLAN). Available: 10.12.1.64/docs/FIE/Asignaturas/Telecomunicaciones y Electrónica/Modelación y Simulación de Redes/Laboratorios.

ÁLVAREZ VALDERAS, R. C. 2010. *Calidad del Servicio de Videoconferencia de la red Corporativa de la Empresa de Telecomunicaciones de Cuba* tesis de maestría, Universidad Central "Marta Abreu" de Las Villas.

AMADO GIMÉNEZ, R. 2008. *Análisis de la Seguridad en Redes 802.11*. Universidad de Valencia.

BARRENECHEA ZAVALA, T. I. 2009. *Diseño de una Red LAN Inalámbrica para una Empresa de Lima.* Pontificia Universidad Católica de Perú.

BARUCH, A. & AMITABH, M. 2008. Introduction to Ad hoc Networks.

BROADCOM, C. 2003. 802.11g :The New Mainstream Wireless LAN Standard.

BUETTRICH, S. & ESCUDERO, P. 2007. Topología e Infraestructura Básica de Redes Inalámbricas. Fundación Escuela Latinoamericana de Redes. Fecha de Actualización.

CABRERA E, C. A. 2007. Wireless LAN: Diseño. Available: http://cesarcabrera.info/1disenno.pdf

CAÑAS, J. Diseño de Redes Inalámbricas. 2004.

CARTAS, M. A. G. 2009. *Descripción de las tecnologías empleadas en las normas IEEE 802.11n y IEEE 802.16e* Trabajo de Diploma, Universidad Central Marta Abreu de Las Villas.

COMMITTEE, I. C. S. L. M. S. 1999. Supplement to IEEE Standard for Information Technology--Telecommunications and Information Exchange Between Systems--Local and Metropolitan Area Networks--Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications:High-speed Physical Layer in the 5 GHz Band. IEEE.

COMMITTEE, I. C. S. L. M. S. 2005. Information technology —Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements:Part 11:Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications IEEE.

COMMITTEE, I. C. S. L. M. S., ELECTRICAL, I. O., ENGINEERS, E. & BOARD, I.-S. S. 2000. Supplement to IEEE Standard for Information Technology--Telecommunications and Information Exchange Between Systems--Local and Metropolitan Area Networks--Specific Requirements: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-speed Physical Layer Extension in the 2.4 Ghz Band. IEEE.

COMMITTEE, L. M. 2007. IEEE Std 802.11-2007: IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Computer Society*.

COMMITTEE, L. M. 2009. IEEE Std 802.11n-2009: IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Enhacements for Higher Throuhput. *IEEE Computer Society*.

COMMUNICATIONS, S. E. 2008. WLAN Security Today: Wireless more Secure than Wired. Available: http://www.enterasys.com/company/literature/wlan%20security%20today-siemens%20whitepaper_en.pdf.

CHÁVEZ, C. N. 2009. *Evaluación de la tecnología IEEE 802.11n con la plataforma OPNET*. Trabajo de Diploma, Universitat Politécnica de Catalunya.

ESCUDERO PASCUAL, A. 2009. Estándares Inalámbricos.

ESPINOSA GIRALDO, R. A. 2011. *Diagnóstico y rediseño de la Red Inalámbrica de la Universidad Católica de Pereira.* Universidad Católica de Pereira,.

FLORES, J. L. G. 2009. *Análisis y diseño de una red LAN inalámbrica para la Empresa Bio-Electrónica Blanco S.A.*, Escuela Politécnica Nacional

GAYAL, S. & MANICKAM, S. A. V. 2003. Wireless LAN Security :Today and Tomorrow

GHETIE, J. 2008. *Fixed-Mobile Wireless Networks Convergence, ,* Cambridge University Press.

GIBSON, J. D. 2002 *The Communications Handbook* CRC Press.

HEMÁNDEZ-SERRANO, J. & PEGUEROLES, J. 2004. Montar un punto de acceso inalámbrico 802.11 en LINUX.

KATZ, M. D. & FITZEK, F. H. P. 2009. *WIMAX Evolution: Emerging Technologies and Applications*, Wiley

KHOSA, I., HAIDER, U. & MOSOOD, H. Evaluating the performance of IEEE 802.11 MAC protocol using OpNET modeler. Electronics and Information Engineering (ICEIE), 2010 International Conference On, 2010. IEEE, V2-91-V2-95.

KUMAR JHA, R. 2010. Performance Comparison of Intelligent Jamming In RF (Physical) LAYER with WLAN Ethernet Router and WLAN Ethernet Bridge. Available: http://www.itu.int/dms_pub/itu-t/oth/29/04/T290400000700710PDFE.pdf.

LEW, M. 2012. LAN inalámbrica 802.11ac. Novedades y su repercusión en el diseño y las pruebas.

MALDONADO ERAZO, W. S. 2009. *Implementación y Configuración de una Red Inalámbrica WLAN y Cámaras de Seguridad IP para Hostal La Carolina.* Escuela Politécnica Nacional

MARTINEZ, D. L. L. R. 2011. SEGURIDAD EN REDES WI-FI.

MENDIGAÑA CASTILLO, D. H. & REINA ASCENCIO, Y. F. 2008. *Diseño, Implementación y Configuración de una Red Inalámbrica en la Corporación Universitaria Minuto de Dios (Girardot).* Corporación Universitaria Minuto de Dios.

MERINERO, J. M. 2010. *Diseño de Infraestructuras de red y soporte informatico para un centro publico de educacion infantil primaria.* Universidad Politécnica de Madrid.

OCHOA CORREA, V. A. 2006. Uso del Packet Tracer y Aplicaciones Resueltas

QUEDNOW M, E. A. 2006. *Diseño e Implementación de una Red Inalámbrica de área Metropolitana, para distribución de Internet en medios suburbano, utilizando el protocolo IEEE 802.11B* Universidad de San Carlos de Guatemala

QUOBIS, N. 2009. WiMAX: la revolución inalámbrica... ¡ y móvil !

ROMERO KANASHIRO, W. R. 2013. Redes inalámbricas y simulación de WLAN mediante OPNET.

ROSAS RAMOS, J. 2006. *Seguridad en redes inalámbricas IEEE 802.11 (WLAN) con WEP mejorado.* Universidad de las Américas Puebla.

SOUNGALO, T. & RENFA, L. 2010. Evaluating and Improving Wireless Local Area Networks Performance.

SUMMARIES, C. 2003. Wireless networks: threats, advantajes and safeguards. Available: http://www.clusif.asso.fr/fr/production/ouvrages/pdf/wlan_eng.pdf.

WATSON, R. 2012. Understanding the IEEE 802.11ac Wi-Fi Standart Meru .

ANEXOS

Anexo I Definición de un nuevo proyecto

Primero se va a **Inicio**, **Todos los programas**, **OPNET Modeler 14.0**, **OPNET Modeler 14.0**

Luego de esto ya se está en la interfaz inicial del OPNET Modeler, aquí se marca **File**, **New**, se elige **Project** entre las diferentes opciones y se marca **OK** , se pone el nombre de el escenario que se quiere crear y del proyecto que en este caso sería el que se muestra en la fig. 2.1.1:

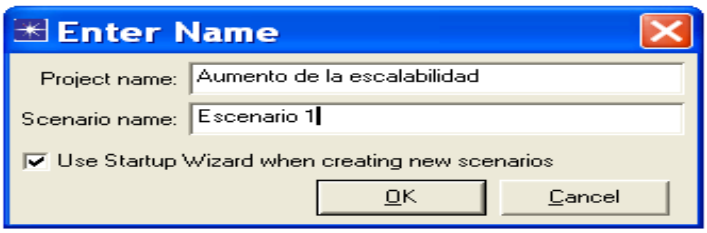


Figura I. 1. Asignación del nombre del proyecto.

Después de marcar **OK** en figura I.1 aparece la ventana Startup Wizard, donde en el caso del proyecto que se llevó a cabo se realizaron las siguientes elecciones en Initial Topology (topología inicial), se marcó **Create empaty scenario** lo cual indica que se creará un escenario vacío para luego incluir en este los elementos a utilizar, en Choose Network Scale (escoja la escala de la red) se marcó **Office**, en Specify Size (especifique el tamaño) se eligió 100 metros de largo y 100 de ancho, en Select Technologies (tecnologías seleccionadas) se eligieron **ethernet** y **wireless_lan_adv** con el objetivo de tener más a mano en la paleta de objetos los dispositivos con que se montarán los escenarios. Después de que se realizaran todos los pasos anteriores la ventana Startup Wizard quedó como se muestra en la siguiente figura:

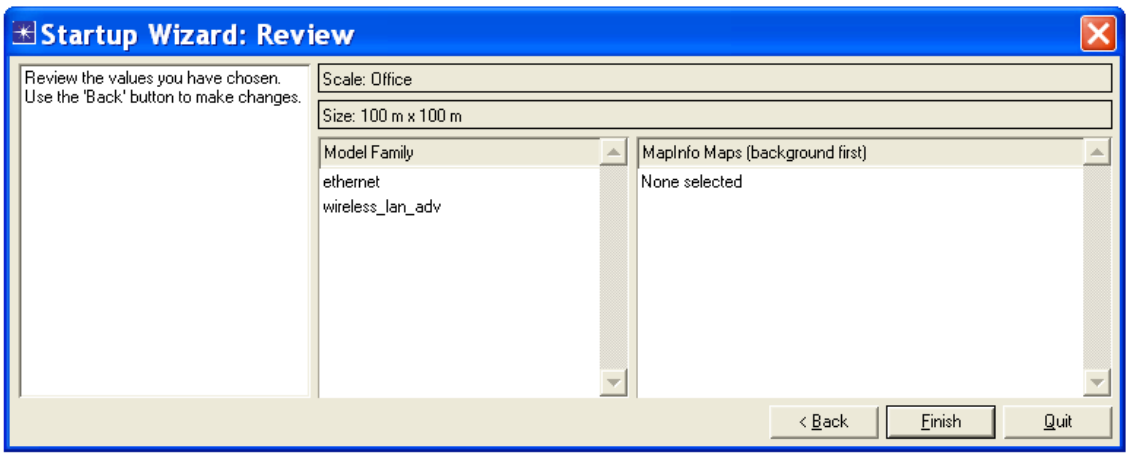


Figura I. 2. Revisión de las opciones seleccionadas.

Esta ventana permite observar las elecciones realizadas en la creación de un nuevo proyecto, si se detecta un error se puede buscar mediante **Back** (atrás) y corregirlo, si no se observan errores se marca **Finish** y entoces queda conformado el nuevo proyecto.

Anexo II Elementos utilizados en la creación de los escenarios

Para la creación de los 4 escenarios se seleccionaron de la paleta de objetos ( ) los siguientes elementos :

- Application Configuration (Configuración de Aplicaciones).

- Profile Configuration (Configuración de Aplicaciones).

- Ethernet_server (servidor ethernet).

- Cisco 2924XL.

- Ethernet_wkst (estación ethernet) .

- Ethernet 100BaseT.

- wlan_wkstn_adv (estación inalámbrica).

- wlan_ethernet_slip4_adv.