Universidad
Carlos III de Madrid

Escuela Politécnica Superior
Ingeniería Técnica de Telecomunicación:
Telemática

Proyecto Fin de Carrera

Evaluación de prestaciones en redes inalámbricas multi-salto con routers Linksys WRT54GL

Autor: Elena Manchón Pérez

Tutor: Ignacio Soto Campos

Leganés, septiembre de 2015

Título: Evaluación de prestaciones en redes inalámbricas multi-salto con routers Linksys WRT54GL
Autor: Elena Manchón Pérez
Director: Ignacio Soto Campos

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Aunque parecía que nunca llegaría el día en el que estuviera escribiendo estas líneas, después de último esfuerzo tardío, las estoy escribiendo.

En primer lugar tengo que dar las gracias a mi tutor Ignacio, por la dedicación y tiempo que me ha dedicado. Contestando rápidamente a todas mis dudas y ayudándome a resolver todos los problemas que han surgido mientras realizaba el trabajo. Sin su ayuda y constancia, me habría sido imposible finalizar este proyecto.

Tengo que dar las gracias a Aitor, que es la persona que me acompaña cada día, que me anima y me apoya. Gracias por tener paciencia conmigo aunque a veces me desespere y hacer sencillo aquello que me parecía inalcanzable.

Dar las gracias a mi familia, que siempre están ahí, y aunque les costó finalmente supieron comprender que debían dejar que finalizara esta carrera por mí misma sin tantas presiones.

También quiero dar las gracias a mis amigas, porque siempre puedo contar con ellas, porque han estado a mi lado en los momentos buenos y en los malos desde hace tantos años.

Y como no podía ser de otro modo, y aunque ya hace tiempo que dejamos las clases, siempre estaré agradecida a mi compañera Sara. Una persona que no solo fue compañera sino también amiga. Y que a día de hoy es el mejor recuerdo que tengo de la universidad.

Resumen

En la actualidad existen multitud de tipologías de redes inalámbricas multi-salto, que están en permanente evolución. Debido a la gran diversidad y heterogeneidad de estas redes, son necesarios estudios que nos aporten información sobre su comportamiento.

En este proyecto se ha realizado un estudio sobre una tipología de red inalámbrica específica cuyos nodos están formados por routers inalámbricos Linksys WRT54GL. Se han contemplado varios escenarios con diferentes saltos inalámbricos, y realizado pruebas con diferentes parámetros para evaluar el comportamiento del througthput y otros parámetros de prestaciones en cada caso.

Se ha realizado una representación gráfica de los resultados obtenidos en las pruebas y sacado conclusiones de su comportamiento.

Para llevar a cabo el estudio se ha realizado una automatización mediante shell script, para facilitar el cambio de parámetros en los routers y la obtención de la salida de información de las pruebas en un formato manejable para su posterior estudio.

Abstract

Keywords: wireless, mesh networks, iee802.11, ad-hoc networks

Wireless mesh networks are a new paradigm that is receiving a lot of attention. In wireless mesh networks traffic may have to go through different wireless hops to reach its destination. Wireless mesh networks often consist of mesh clients, mesh routers and gateways.

In this work, we have tested the performance of different wireless network topologies, with different number of routers and wireless hops. The wireless technology used is based on the IEEE 802.11 specifications, specifically in the 2.4 Ghz frequency band (802.11b and 802.11g amendments of 802.11).

We have carried out experiments modifying different parameters besides the network topology, for example UDP packet size, frequency channel or routers' transmit power. In the experiments we measure throughput and packet losses to evaluate the achieved performance. The configuration of the parameters to be used in each experiment was automatized in order to simplify data gathering and analysis.

Índice general

Índice de figuras

Índice de tablas

1. Introducción al Proyecto

1.1 Motivación

Vivimos en una era en la que el mundo de la portabilidad está a la orden del día, ya no imaginamos qué haríamos sin nuestro móvil, nuestro portátil o nuestra Tablet. Usamos dispositivos móviles, en nuestro ocio, en nuestro trabajo o en muchas otras circunstancias. Nos permiten realizar muchas actividades como buscar un hotel, ver las recomendaciones de un restaurante cuando vamos de viaje, consultar nuestra cuenta corriente o realizar una operación bancaria en cualquier sitio, mantener reuniones de trabajo fuera de nuestra oficina, o controlar y monitorizar nuestra actividad empresarial. Todo esto es posible gracias a una nueva generación de dispositivos basada en los muchos avances que se han hecho en la última década en la tecnología de redes inalámbricas.

Las redes inalámbricas nos permiten una flexibilidad y movilidad anteriormente impensable. A pesar de que es una tecnología muy afianzada todavía sigue en continua evolución llegando ya a velocidades comparables con las redes cableadas de hace unos pocos años.

El Instituto de Ingeniería Eléctrica y Electrónica (*Institute of Electrical and Electronics Engineers, conocido por sus siglas* ***IEEE)*** ha definido las especificaciones 802.11 [**1**], un conjunto de estándares que extienden el estándar de red local Ethernet cableada al dominio inalámbrico, es decir, define las características de una red de área local inalámbrica *(WLAN*). Los estándares 802.11 son ampliamente conocidos como "Wi-Fi", porque la *Wi-Fi Alliance*, anteriormente WECA *(Wireless Ethernet Compatibility Alliance)*[**2**] ofrece certificación para productos 802.11, garantizando que un producto cumple con los estándares 802.11.

En la actualidad, no solo nos encontramos redes inalámbricas de infraestructura, donde hay un único salto inalámbrico al punto de acceso (AP), sino que hay una tendencia hacia redes inalámbricas con múltiples saltos inalámbricos. Estas redes multi-salto, permiten mayor flexibilidad, pero pueden llevan una penalización de rendimiento, siendo mayor cuantos más saltos inalámbricos nos encontremos. Es importante llevar a cabo un estudio del comportamiento y prestaciones de redes inalámbricas multi-salto, para poder evaluar las ventajas frente a los inconvenientes de estas redes y así poder crear infraestructuras óptimas. Ejemplos de redes multi-salto serían las redes mesh o malladas o las recientes redes vehiculares.

En este proyecto se han realizado comparativas con diferentes saltos inalámbricos para poder ver cómo afecta al rendimiento cada escenario. Los estándares sobre los que se han creado estos escenarios, son el 802.11b y el 802.11g.

1.2 Objetivos

En los últimos años se ha incrementado notablemente el interés por las redes ad-hoc que permiten a los usuarios de dispositivos móviles con tecnología inalámbrica conectarse entre sí sin necesidad de usar la infraestructura de un tercero para intercambiar información entre ellos. Igualmente importante hoy en día es el interés en usar redes ad hoc para conectarse a la infraestructura, pero sin necesidad de estar directamente conectados a un nodo en dicha infraestructura, sino poder llegar a él a través de varios saltos inalámbricos.

La creación de nuevas redes multi-salto, donde no se depende de un nodo central al que conectarse, sino que cada nodo puede comunicarse con los demás, permite una flexibilidad y una robustez muy interesantes. Pero al añadir un mayor número de saltos inalámbricos el rendimiento puede deteriorarse. Es necesario estudiar el comportamiento de esta tipología de red, para poder encontrar un equilibrio entre las ventajas que nos ofrecen y la pérdida de rendimiento.

El objetivo de este proyecto es la evaluación de prestaciones de redes inalámbricas 802.11 en la banda de 2,4 GHz (estándares 802.11b y 802.11g) y el efecto de incluir múltiples saltos inalámbricos. Se trata de realizar la medición de una serie de parámetros para evaluar la calidad y el rendimiento de la conexión inalámbrica y realizar una comparativa con diferentes escenarios creados por la composición de varios saltos inalámbricos, conseguidos por la inclusión de uno o más routers.

Se quería conseguir una adecuada caracterización de las prestaciones mediante parámetros como throughput TCP, pérdidas de paquetes UDP, etc. Para ello se realizaron mediciones con equipos reales, obteniendo medias e intervalos de confianza resultado de varias ejecuciones de los experimentos.

Para simplificar el proceso de cambio de parámetros y toma de resultados, un requisito adicional era crear un sistema de automatización de pruebas.

1.3 Estructura del proyecto

La presente memoria del proyecto está estructurada como se expone a continuación:

- ***Capítulo 1: Introducción:***

Este capítulo. En él se hace una primera toma de contacto con el tema que se va a tratar a lo largo del proyecto. Se explica la motivación del proyecto y los objetivos que se plantearon en un inicio.

- ***Capítulo 2: Introducción a las redes inalámbricas WLAN***

Presentación de las tecnologías usadas en el proyecto.

  - *Capítulo 2.1*: Introducción a las redes inalámbricas

Breve explicación de las redes inalámbricas WLAN

  - *Capítulo 2.2*: Ventajas e Inconveniente

Enumeración y descripción de los puntos positivos y negativos de las redes inalámbricas.

  - *Capítulo 2.3: Tipologías*

Descripción de las principales infraestructuras de redes WLAN que podemos encontrarnos.

  - Capítulo 2.4: Estándares 802.11

Descripción de los estándares 802.11 haciendo hincapié en los utilizados en el proyecto.

  - Capítulo 2.5: Evaluación de prestaciones en redes inalámbricas

Descripción de algunos ejemplos de uso de redes inalámbricas y la importancia de su continuo estudio.

  - Capítulo 2.6: Conclusiones

Unas breves conclusiones de lo visto en el capítulo.

- ***Capítulo 3: Diseño del Proyecto***

    - Capítulo 3.1: Listado de los parámetros de rendimiento

Enumeración y descripción de los parámetros seleccionados para medir el rendimiento en las redes inalámbricas estudiadas.

    - Capítulo 3.2: Listado de las herramientas a utilizar

Enumeración y descripción de algunas de las herramientas existentes para realizar las mediciones.

    - Capítulo 3.3: Elección de las herramientas a utilizar

Listado de las posibles herramientas que podrían aplicarse para nuestro estudio y la elección de las que se consideran más adecuadas para este proyecto.

    - Capítulo 3.4: Descripción de la infraestructura

Descripción de los elementos utilizados y los escenarios utilizados para las pruebas.

- ***Capítulo 4: Automatización***

    - *Capítulo 4.1: Cambio de parámetros en los routers*

Detalle de script realizado para automatizar el cambio de parámetros en cada router implicado en la pruebas.

    - *Capítulo 4.2: Recogida datos latencia*

Detalle de script realizado para automatizar la recogida de la latencia obtenida en las pruebas.

    - *Capítulo 4.3: Recogida datos pruebas TCP y UDP*

Detalle de script realizado para automatizar la recogida de los datos más relevantes resultado de las pruebas realizadas con TCP y UDP.

- ***Capítulo 5: Pruebas***

Descripción de los escenarios y pruebas realizadas en cada uno de ellos, las conclusiones obtenidas y los scripts de automatización realizados.

  - *Capítulo 5.1: Escenarios*

Descripción de los diferentes escenarios evaluados.

  - *Capítulo 5.2: Pruebas*

Detalle de las pruebas realizadas.

  - *Capítulo 5.3: Resultados*

Gráficas de los resultados obtenidos en las pruebas y su descripción. Los resultados se han clasificado según los diferentes escenarios y casuísticas más representativas.

  - *Capítulo 5.4: Conclusiones pruebas*

Enumeración de las conclusiones obtenidas de las pruebas realizadas.

- ***Capítulo 6: Conclusiones***

Dictamen final con las conclusiones del estudio realizado.

- ***Capítulo 7: Futuras líneas de trabajo***

Descripción de las futuras líneas de trabajo que pueden seguirse para completar el estudio.

2. Redes inalámbricas WLAN

Pueden encontrarse diferentes tipologías de redes inalámbricas. En este capítulo vamos a realizar una breve descripción de alguna de estas redes y contrastar las ventajas e inconvenientes frente a una red cableada.

2.1 Introducción redes inalámbricas

A pesar de que no son las redes con las que vamos a trabajar en este proyecto pasamos a detallar un pequeño resumen de algunas otras opciones de red inalámbrica que podemos encontrar.

Redes inalámbricas de área personal (WPAN)

Tienen en general un alcance bastante limitado. Las tres principales tecnologías de este tipo de redes son:

- *Bluetooth*

Lo incluyen todos los ordenadores portátiles y teléfonos móviles modernos. Su radio de acción varía entre 1 y 100 metros. Lo normal es que ronde unos 10. Ofrece velocidades entre 1 y 3 Mbps, aunque la versión de Bluetooth 3.0 + HS podrá alcanzar los 24 Mbps.

- *ZigBee:*

Se usa sobre todo en el entorno industrial o empresarial y en aplicaciones de domótica (casas "inteligentes"). Porque es barato, consume muy poco y es bastante resistente a las interferencias.

No está diseñado para grandes velocidades de transferencia. Oscila entre 20 y 250 kbps, muy por debajo del Bluetooth. El alcance normal es similar, aunque el ZigBee Pro puede llegar a 1.600 metros en condiciones ideales.

- *Infrarrojo*

Es la tecnología que usan los mandos a distancia de siempre. Hubo una época en que se incluía en ordenadores portátiles u otros dispositivos móviles. En la actualidad se ha sustituido en gran medida por el Bluetooth.

Las redes inalámbricas de infrarrojo no funcionan a través de objetos sólidos como las paredes. Su alcance normal es menor que el del Bluetooth o

el ZigBee. Además, el emisor y el receptor tienen que "verse" mutuamente para que la transmisión sea posible.

La velocidad varía mucho de unos tipos a otros. Con un mínimo de sólo unos pocos kbps hasta un máximo de 16 Mbps.

Redes celulares

Las redes celulares son redes formadas por celdas de radio cada una con su propio transmisor, conocido como estación base. Las celdas están alineadas unas al lado de otras en un formato similar a un panal de abejas, por este motivo se conocen como redes celulares.

La telefonía móvil utiliza este tipo de redes inalámbricas. Un teléfono móvil debe tener a la vista alguna de las estaciones base de telefonía móvil. Cada estación base sólo puede trasmitir una cantidad finita de llamadas. En zonas de alta utilización de teléfonos móviles, tales como el distrito central de negocios y las zonas de alta densidad de población, se requieren más estaciones base para manejar el nivel de tráfico de llamadas.

Las llamadas pueden transferirse de una estación base a otra, por lo que si el usuario se sale de la celda en la que se encuentra, el teléfono móvil automáticamente buscará la señal de una estación base adyacente.

Cada estación de telefonía móvil debe distinguir la señal de un transmisor del resto de señales de otros transmisores. Para ello hay varias soluciones, como pueden ser **FDMA** (*Frecuency Division Multiple Access*), **CDMA** (*Code Division Multiple Access*) y **TDMA** (*Time Division Multiple Access).*

Redes inalámbricas de área local (WLAN)

En el primer capítulo se hizo una breve referencia a estas redes, ya que son las redes sobre las que se ha trabajado. Como ya se comentó están estandarizadas por el Instituto de Ingenieros en Electricidad y Electrónica (IEEE), concretamente en la familia de estándares 802.11. Este estándar nace para facilitar la conectividad de estaciones fijas, portátiles o móviles dentro de un área local.

Una red WLAN se trata de una red de área local inalámbrica, donde en lugar del par trenzado, coaxial o fibra óptica utilizada en las LAN convencionales, se transmite y reciben los datos utilizando tecnología de radiofrecuencias. Estas redes suelen tener muy buena calidad de emisión en

distancias cortas (en teoría 100m) y proporciona una conectividad inalámbrica de igual a igual (*peer to peer*). Este tipo de redes se usan habitualmente dentro de un edificio, de una pequeña área residencial/urbana o de un campus universitario, por ejemplo. En el capítulo 2.4 se detallan en mayor profundidad.

Para la transmisión es necesario el uso de antenas integradas en las tarjetas. Además este tipo de ondas son capaces de traspasar obstáculos sin necesidad de tener visión directa el emisor y el receptor.

2.2 Ventajas e inconvenientes

A continuación se detallan los beneficios del uso de una red inalámbrica:

- **Fácil instalación**: Una de las ventajas principales del uso de redes inalámbricas es su fácil instalación debido a la ausencia de cables, lo permite su utilización en espacios de logística compleja en los que resulte difícil establecer el cableado.

- **Abaratamiento**: El hecho de no necesitar un tendido de cables abarata los costes.

- **Versatilidad**: Permite ampliar o trasladar de una manera sencilla y rápida, la infraestructura.

- **Movilidad**: Dota de libertad de movimientos a todos los dispositivos conectados a la red.

- **Sencillez**: No aumenta la complejidad al conectar más dispositivos.

- **Mayor expansión**: Permite crear una red en áreas complicadas donde, por ejemplo, resulta dificultoso o muy caro conectar cables.

Evidentemente, no todo son ventajas, las redes inalámbricas también tiene unos puntos negativos en su comparativa con las redes de cable. Los principales inconvenientes de las redes inalámbricas son los siguientes:

- **Menor ancho de banda.** A pesar de la gran evolución que ha habido respecto al ancho de banda de estas redes, se mantiene por detrás de los estándares cableados.

- **Mayor inversión inicial.** Para la mayoría de las configuraciones de la red local, el coste de los equipos de red inalámbricos es superior al de los equipos de red cableada.

- **Seguridad**. Al no necesitar de un medio físico para funcionar, cualquier persona con el equipo adecuado puede acceder a la red simplemente estando en el área de cobertura, esto permite flexibilidad pero también es un riesgo para la seguridad de la red. Además el hecho de que la cobertura no esté definida o limitada por paredes u otro medio físico, permite a los posibles intrusos no estar ni siquiera en el mismo edificio. Este problema ha mejorado mucho con las certificaciones de seguridad WPA y WPA2 basadas en normas de la WI-FI Alliance que proporcionan autenticación mutua para verificar a usuarios individuales y cifrado avanzado.

- **Interferencias**. Las redes locales inalámbricas usan espectro radioeléctrico en bandas de uso sin licencia lo que implica que puede ser utilizada por otros muchos equipos del mercado, como otras redes inalámbricas, teléfonos inalámbricos, microondas, etc. Este hecho hace que no se tenga garantía de que la franja de frecuencia que estemos utilizando este libre para que nuestra conexión inalámbrica funcione en su mayor rendimiento.

  Además nos encontramos con un número limitado de canales de frecuencia. Si la red inalámbrica trabaja en la banda de frecuencia de 2,4 GHz, que es la más común, solo existen 11 canales disponibles, que al tener solapamiento entre ellos, realmente dejan disponible tres de ellos para un uso óptimo.

  Cuanto mayores sean las interferencias producidas por otros equipos, menor será el rendimiento de nuestra red. No obstante, el hecho de que haya probabilidades de sufrir interferencias no quiere decir que sean tan graves como para que la conexión sea inaceptable. La mayoría de las redes inalámbricas funcionan perfectamente sin mayores problemas en este sentido.

- **Instalación/gestión.** A pesar de que se ha incluido como ventaja la fácil instalación de redes inalámbricas, la instalación y gestión se complica cuando se trata de redes permanentes que requieren garantizar un nivel de cobertura adecuado. Temas como la elección de la situación de los puntos de acceso, la seguridad, la selección de los canales u otros parámetros avanzados de configuración, terminan complicando la instalación y gestión de una red inalámbrica por encima de una cableada. Las interferencias además pueden cambiar degradando las prestaciones, lo que obliga a una monitorización más exhaustiva que en una red cableada.

2.3 Tipologías

En función de los elementos que participen y la manera de conectarse podemos tener las siguientes tipologías:

Red ad hoc

Una red inalámbrica ad hoc es una red compuesta por dispositivos móviles de computación que usan la transmisión inalámbrica para comunicarse sin tener ningún tipo de infraestructura fija (sin dispositivos de administración centralizada, tales como las estaciones base de las redes inalámbricas celulares o los puntos de acceso de las redes inalámbricas de área local).

En esta tipología los nodos se conectan directamente entre sí inalámbricamente de modo que cada nodo forma parte de una red *peer to peer (conocida por el acrónimo P2P).* Por lo tanto, en las redes ad hoc los nodos clientes se conectan directamente entre ellos, ver ejemplo en la *Figura 1*. Es una red descentralizada, donde cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos. Solamente los nodos dentro de un rango de transmisión definido pueden comunicarse entre ellos.

Permite la adhesión de nuevos nodos a la red simplemente con estar en el rango de cobertura. Cada nodo puede conectar con el resto de nodos dentro de su cobertura para formar una red punto a punto en la que cada equipo actúa como cliente y como punto de acceso simultáneamente.

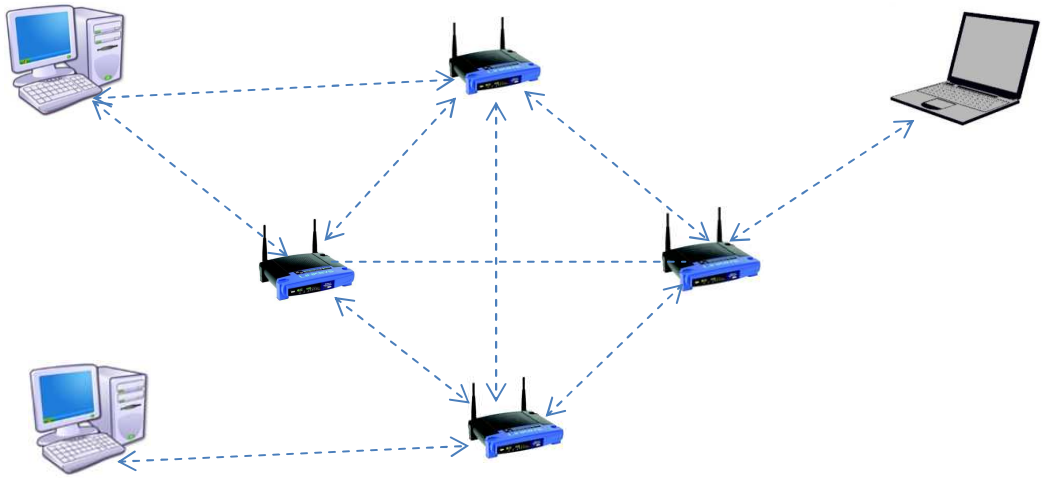
Al tratarse del modo más sencillo para formar una red, ya que no se requiere una infraestructura específica, es recomendable para redes creadas de forma espontánea en un tiempo y espacio limitado.

Dado que cada nodo puede ser un salto más por el que viaja la información, esto puede ser uno de los principales inconvenientes ya que cuantos más saltos de la información más retardo conllevará y más probabilidad de sufrir un error o se corrompa.

La conexión entre los nodos está limitada por los recursos de dichos nodos, como por ejemplo la potencia de transmisión, la potencia de cálculo y memoria, y las propiedades de comportamiento (ej: fiabilidad), así como de las propiedades de enlace (ej: la duración de la conexión, pérdida de señal, interferencia y ruido). En la exposición del diseño del proyecto se han detallado estas propiedades ya que muchas de ellas se han tenido en cuenta para el

estudio de las prestaciones de los routers a evaluar, ya que se ha utilizado esta topología de red.

Figura 1. Ejemplo sencillo de red ad hoc



Red con infraestructura

Este tipo de redes se caracterizan por tener un equipo especializado, llamado punto de acceso (AP), al que se conectan sin cables el resto de dispositivos. Estas redes suelen extender una red LAN cableada ya existente, donde el AP sirve de puente entre ambas redes coordinando la transmisión y recepción de los diferentes dispositivos inalámbricos.

Esta red de tipo cliente-servidor es la más extendida actualmente, donde el ejemplo más habitual es que los clientes son ordenadores personales, móviles o tablets, que obtienen acceso a la red a través del AP.

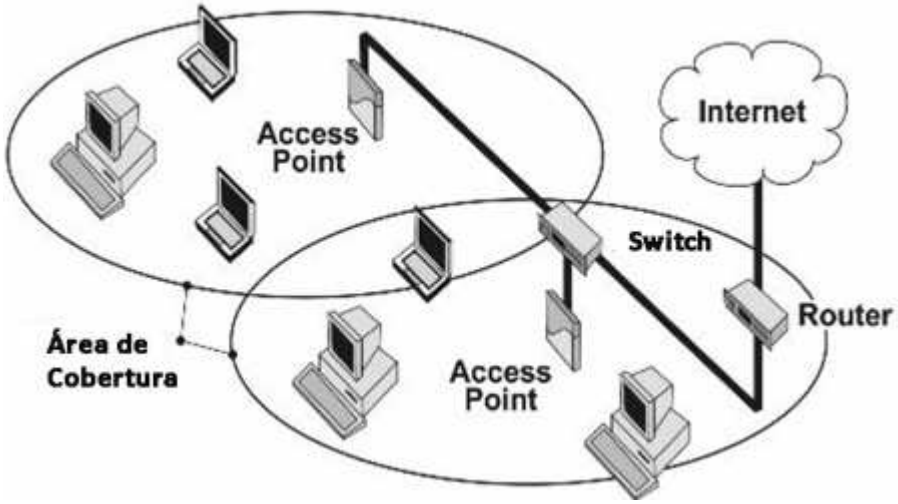
Los puntos de acceso se identifican con un identificador único llamado BBSID (*Basic Service Set IDentifier*), y normalmente también por su ESSID (*Extended Service Set ID*) que es el nombre identificable de la red. El BSSID coincide con la dirección MAC del punto de acceso.

Al contrario que las redes ad hoc, estas redes son centralizadas ya que para conectar un cliente con otro, deben comunicarse a través del punto de acceso. Uno de los mayores inconvenientes de esta gestión centralizada es

que si se cae el punto de acceso cada terminal de red queda incomunicado. La zona de cobertura es aquella que proporciona el punto de acceso, siendo esta también una de las limitaciones.

En la *Figura 2* puede verse un ejemplo sencillo con dos puntos de acceso y su área de cobertura.

Figura 2. Ejemplo de red con infraestructura



Fuente: http://foro.tecnicasprofesionales.com/index.php?topic=788.0
[Consulta 18-09-2015]

Redes malladas

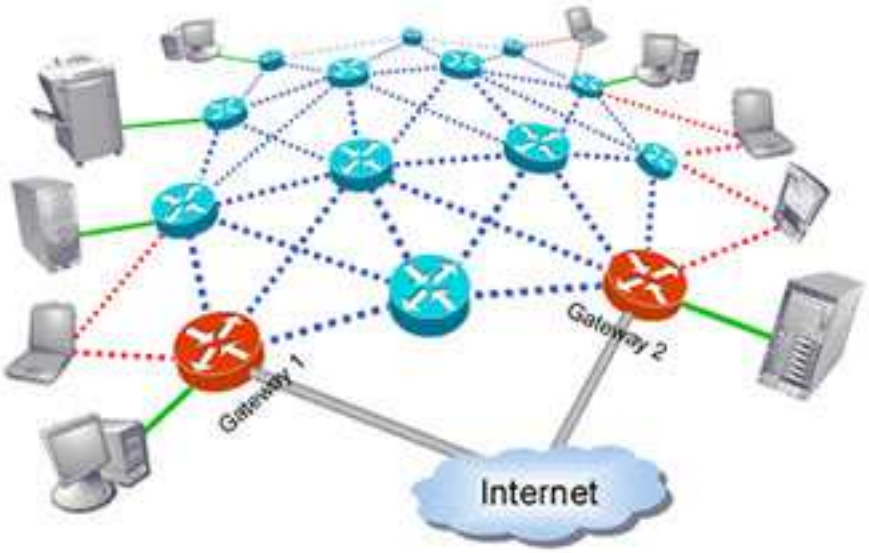
Las redes malladas o mesh, son aquellas en las que sus enlaces son inalámbricos y los nodos pueden actuar como host (cliente mesh), como router (router mesh), o como ambas cosas a la vez. Un router mesh reenvía paquetes de otros nodos, que pueden no estar dentro de su cobertura de transmisión directa inalámbrica. Entonces, en una red mallada los nodos pueden comunicarse con nodos que no están en su radio de cobertura, consiguiéndolo gracias al reenvío de paquetes por otros nodos a través de múltiples saltos inalámbricos.

Para simplificar el despliegue de una red mesh, puede tener funciones de auto-configuración y auto-organización, con nodos que se conectan a la red automáticamente, manteniendo una conectividad en forma de malla entre ellos.

Al existir más de un camino para comunicar dos nodos, estas redes tienen mucha fiabilidad y robustez, siendo mayor cuantos más nodos se encuentran configurados dentro de la misma red.

Una red mallada típicamente tendrá conexiones con la infraestructura en determinados nodos, facilitando así el acceso a la infraestructura (a Internet) a todos los nodos de la red mallada. Un ejemplo de ello puede verse en la *Figura 3.*

Figura 3. Ejemplo de red mallada



Fuente: http://telefor.net/wp-content/uploads/2015/04/10.jpg
[Consulta 18-09-2015]

Ejemplos redes inalámbricas multi-salto

En la actualidad pueden encontrarse múltiples aplicaciones de redes multi-salto, como por ejemplo las redes de sensores. Estas redes se basan en dispositivos de bajo coste y consumo (en los nodos) que son capaces de obtener información de su entorno, procesarla localmente, y comunicarla a través de enlaces inalámbricos hasta un nodo central de coordinación.

La red de sensores inalámbricos está formada por numerosos dispositivos, que utilizan sensores para controlar diversas condiciones en distintos puntos, entre ellas la temperatura, el sonido, la vibración, la presión y movimiento o los contaminantes.

Otro ejemplo de red inalámbrica multi-salto, son las redes vehiculares [**3**], o VANET (*Vehicular Ad hoc Network*). Este tipo de redes permite el intercambio de información entre los usuarios que se encuentran en sus vehículos circulando así como el intercambio de información desde y hacia los

proveedores de servicios que poseen estaciones base colocadas a lo largo de las carreteras.

La velocidad de los vehículos en estas redes hacen que sean muy dinámicas y estén en constante cambio, lo que dificulta la realización de comunicaciones efectivas frente a otros tipos de redes malladas más estáticas.

2.4 Estándares 802.11

En este capítulo se detalla una introducción al estándar 802.11, las bandas de frecuencia en las que trabaja (2,4GHz y 5GHz) y se profundiza en las especificaciones más relevantes para este proyecto.

2.4.1 Introducción al estándar 802.11

El estándar 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento para una red local inalámbrica (WLAN). Los protocolos de la rama 802.x definen la tecnología de redes de área local y redes de área metropolitana.

- La **capa física** (a veces abreviada capa "PHY") ofrece tres tipos de codificación de información.

- La **capa de enlace** de datos compuesta por dos subcapas: control de enlace lógico (LLC) y control de acceso al medio (MAC).

La capa física define la modulación de las ondas de radio y las características de señalización para la transmisión de datos mientras que la capa de enlace es responsable de la transferencia fiable de información a través de un circuito de transmisión de datos, controla como los datos se ubican en los medios y son recibidos desde los medios usando técnicas como control de acceso al medio y detección de errores.

El primer estándar que surge es el 802.11 (en 1997), el cual sienta las bases tecnológicas para el resto de la familia. No tuvo apenas relevancia por la baja velocidad binaria (“*bitrate*”) alcanzada, cerca de 2 Mbps, y la carencia de mecanismos de seguridad de las comunicaciones. Muy poco después se publica el 802.11b, el cual es acogido con un gran éxito comercial. Opera en la banda de los 2,4 GHz y permite alcanzar velocidades binarias teóricas de 11 Mbps mediante el empleo de mecanismos de modulación de canal y protección

frente a errores bastante robustos, aunque en la práctica es difícil superar un ancho de banda efectivo de 7 Mbps. Cuando el canal de transmisión es ruidoso, posee un mecanismo de negociación que reduce la velocidad binaria en escalones predefinidos, aumentando paralelamente la robustez de los mecanismos de protección frente a errores. Para complementar su operativa, incorpora un protocolo de seguridad de las comunicaciones, el WEP *o Wired Equivalent Privacy* (privacidad análoga a redes cableadas), habida cuenta de la imposibilidad de confinar las emisiones en un medio más protegido como es el cable en el caso de las redes fijas. Desafortunadamente, el pretencioso nombre no se corresponde a la realidad, pues muy poco después de su publicación se descubrieron importantes defectos que permitían la intrusión en las comunicaciones con escaso esfuerzo y un equipo convencional.

Pese a lo anterior, el éxito fue de tal magnitud que aceleró la creación de nuevos estándares y reclamó una especial atención por entidades de regulación, que empezaron a valorar la ampliación del espectro para este tipo de usos. El siguiente estándar fue el 802.11a, el cual tiene la particularidad de operar a un mayor *bitrate* (teóricamente hasta 54 Mbps) mediante unos esquemas de codificación de canal más sofisticados y sobre bandas en los 5 GHz. Sin embargo, históricamente las instalaciones de 802.11a se limitaron a entornos corporativos debido a su alto coste de *hardware*.

A continuación se muestra una tabla de la familia de especificaciones que se consideran más interesantes desarrolladas por la IEEE para tecnologías de redes WLAN y posteriormente se describen brevemente cada una de ellas.

Tabla 1: Especificaciones del estándar 802.11

IEEE 802.11	
Grupo de trabajo	**Enfoque**
802.11a	54 Mbps WLAN en la banda 5GHz
802.11b	11 Mbps WLAN en la banda 2.4 GHz
802.11g	54 Mbps WLAN en la banda 2.4 GHz
802.11n	Nueva generación de redes WLAN de al menos 100 Mbps
802.11e	QoS y extensiones se utilizan con de 802.11a/g/h
802.11k	Intercambio de información de capacidad entre clientes y AP
802.11s	Define una arquitectura y un protocolo para redes Mesh
802.11v	Mejora la cantidad de energía requerida en los equipos.
802.11ac	Mejora 802.11n, amplia el ancho de banda hasta 160 MHz

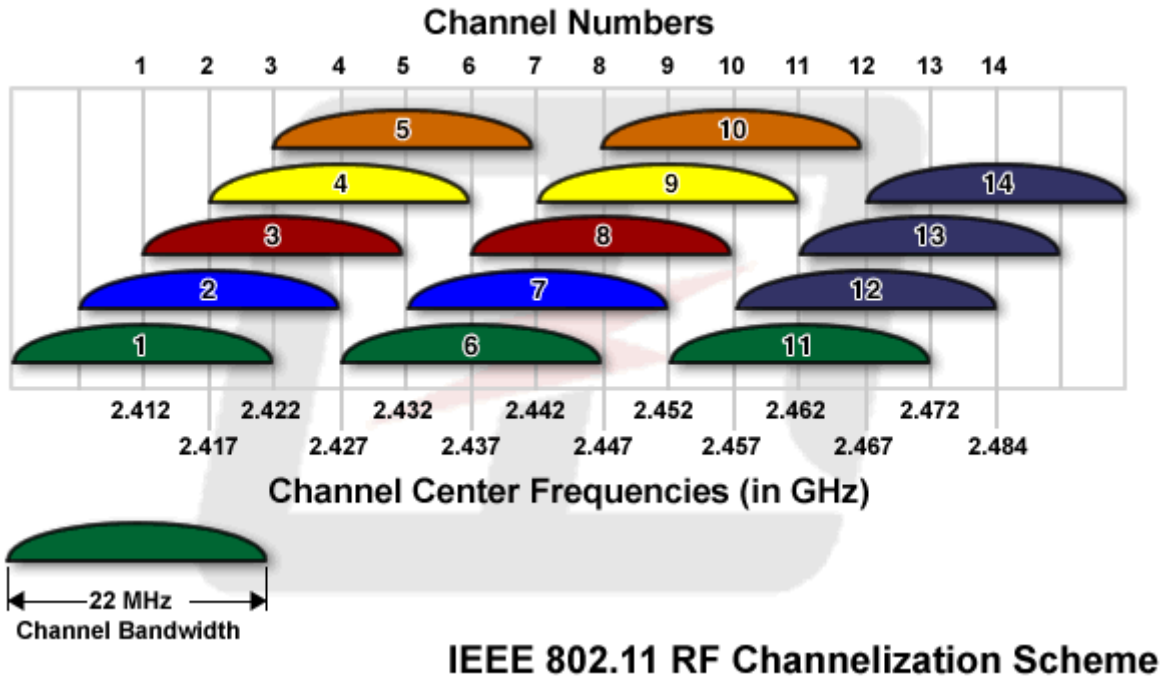
2.4.2 Canales en 802.11

Banda de 2,4GHz

Esta es la banda de frecuencia en la que se trabaja en los estándares 802.11b y 802.11g. En esta banda, cada canal necesita un ancho de banda de 22 Mhz para transmitir la información, por lo que se produce un inevitable solapamiento de varios canales contiguos. Es decir, cada uno de los 14 canales asignados al IEEE 802.11 tiene un ancho de banda de 22 Mhz, y la gama de frecuencias disponible va de los 2.412 GHz hasta los 2.484 GHz. Este espacio es dividido por el IEEE 802.11 en 14 canales, es decir, si bien cada canal es de 22 Mhz, para la totalidad de los 14 canales estamos asignando tan solo 72 MHz en lugar de los 308 MHz necesarios. Para evitar interferencias en presencia de varios puntos de acceso cercanos, estos deberían estar en canales que no se solapan.

En la siguiente imagen se muestra como canales próximos causan interferencia entre sí, pues en la frecuencia del 2.4 GHz solo hay tres canales completos (1, 6 y 11) y los demás se solapan entre sí, es decir, dos canales no completos y contiguos comparten algunas frecuencias:

Figura 4: Información de canales para redes 802.11b/802.11g



Fuente: http://www.amertradela.com/soporte.php
[Consulta 18-09-2015]

Tabla 2: Canales IEEE 802.11b/g

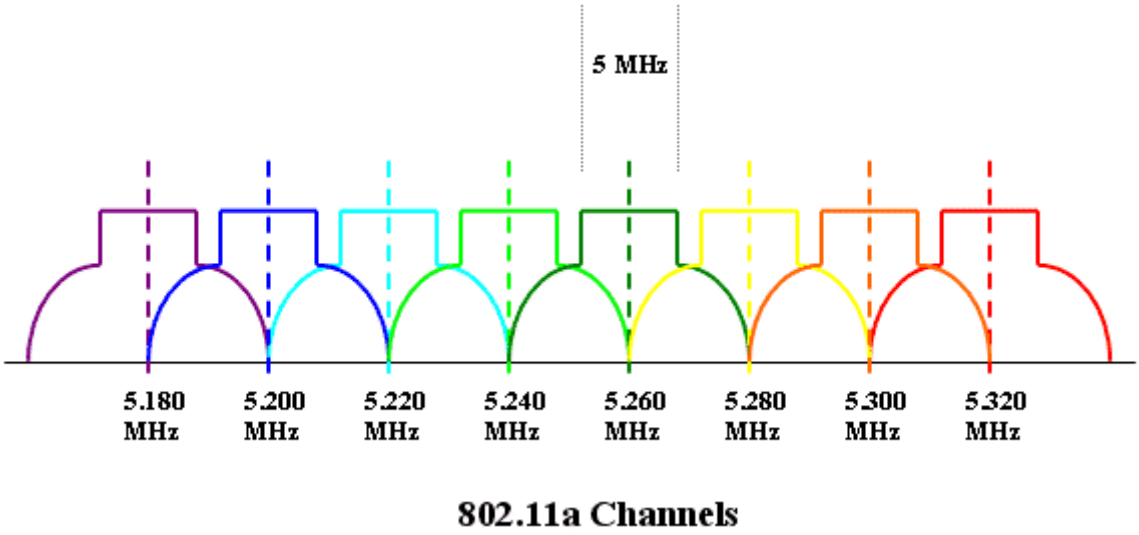
Frecuencia	Canal
2412.0 MHz	1
2417.0 MHz	2
2422.0 MHz	3
2427.0 MHz	4
2432.0 MHz	5
2437.0 MHz	6
2442.0 MHz	7
2447.0 MHz	8
2452.0 MHz	9
2457.0 MHz	10
2462.0 MHz	11
2467.0 MHz	12
2472.0 MHz	13
2484.0 MHz	14

Banda de 5GHz

Esta banda de frecuencia es en la que opera el estándar 802.11a. Utiliza 52 subportadoras *orthogonal frequency-division multiplexing* (OFDM) con una

velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales sin solape. Puede verse una representación en la *Figura 5.*

Figura 5: Canales 802.11a



Fuente: http://www.amertradela.com/soporte.php
[Consulta 18-09-2015]

A continuación se resumen la familia de especificaciones centrándonos en las que se han considerado más interesantes para el concepto de este proyecto.

2.4.3 Familia de estándares 802.11

- **802.11a**

Sus principales características serían:

- Velocidad máxima de hasta 54Mbps
- Opera en un espectro de 5GHz
- Menos saturado
- No es compatible con las normas 802.11b y 802.11g
- Modulación de OFDM.

La revisión 802.11a fue aprobada en 1999 y en 2001 se lanzaron al mercado los productos con este estándar. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz cuya descripción ya se ha realizado previamente. Dado que la banda de 2,4GHz tiene un gran uso, el beneficio de trabajar con la de 5GHz es la reducción de interferencias, pero cuenta con la desventaja de no ser compatible con los equipos que operan con 802.11b o 802.11g, además de que, al ser frecuencias mayores, la distancia de propagación y especialmente la capacidad de atravesar obstáculos se reduce en comparación con los equipos que operan a 2,4 GHz

- **802.11b**

Sus principales características serían:

- Velocidad máxima de hasta 11Mbps
- Opera en un espectro de 2,4GHz
- Utiliza el mismo método de acceso definido en el estándar original CSMA/CA.

En julio de 1999, la IEEE expandió el 802.11 creando la especificación 802.11b, la cual tiene una velocidad teórica máxima de transmisión de 11 Mbit/s, comparable a una Ethernet tradicional, pero debido al espacio ocupado por la codificación del protocolo CSMA/CD (*Carrier Sense Multiple Access / Collision Detect*), en la práctica la velocidad máxima de transmisión es de aproximadamente 5.9 Mbit/s para TCP y 7.1 Mbit/s para UDP. La 802.11b utiliza la misma frecuencia de radio que el tradicional 802.11 (2.4GHz).

- **802.11g**

En junio de 2003, se ratificó un tercer estándar de modulación: 802.11g, que es la evolución de 802.11b. Este utiliza la banda de 2,4 Ghz (al igual que 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, que en promedio es de 22,0 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b.

Sus principales características serían:

- Velocidad máxima de hasta 54Mbps
- Opera en un espectro de 2,4GHz
- Modulación de OFDM.
- Compatible con los equipos 802.11b

Interacción de 802.11g y 802.11b.

802.11g tiene la ventaja de poder coexistir con los estándares 802.11a y 802.11b, esto debido a que puede operar con las Tecnologías RF DSSS y OFDM. Sin embargo, si se utiliza para implementar usuarios que trabajen con el estándar 802.11b, el rendimiento de la celda inalámbrica se verá afectado por ellos, permitiendo solo una velocidad de transmisión de 22 Mbps. Esta degradación se debe a que los clientes 802.11b no comprenden OFDM.

Suponiendo que se tiene un punto de acceso que trabaja con 802.11g, y actualmente se encuentran conectados un cliente con 802.11b y otro 802.11g, como el cliente 802.11b no comprende los mecanismos de envío de OFDM, el cual es utilizado por 802.11g, se necesitará utilizar un mecanismo de compatibilidad, obligando a enviar un RTS/CTS reduciendo la eficiencia.

Suponiendo que el cliente 802.11b no se encuentra conectado actualmente, el Punto de acceso envía tramas que brindan información acerca del Punto de acceso y la celda inalámbrica. Sin el cliente 802.11b, en las tramas se verían la siguiente información:

NON_ERP present: no
Use Protection: no

ERP (Extended Rate Physical), esto hace referencia a dispositivos que utilizan tasas de transferencia de datos extendidos, en otras palabras, NON_ERP hace referencia a 802.11b. Si fueran ERP, soportarían las altas tasas de transferencia que soportan 802.11g.

Cuando un cliente 802.11b se asocia con el AP (Punto de acceso), éste último alerta al resto de la red acerca de la presencia de un cliente NON_ERP. Cambiando sus tramas de la siguiente forma:

NON_ERP present: yes
Use Protection: yes

Ahora que la celda inalámbrica sabe acerca del cliente 802.11b, la forma en la que se envía la información dentro de la celda cambia. Ahora cuando un cliente 802.11g quiere enviar una trama, debe advertir primero al cliente 802.11b enviándole un mensaje RTS (Request to Send) a una velocidad de 802.11b para que el cliente 802.11b pueda comprenderlo. El mensaje RTS es enviado en forma de unicast. El receptor 802.11b responde con un mensaje CTS (Clear to Send).

Ahora que el canal está libre para enviar, el cliente 802.11g realiza el envío de su información a velocidades según su estándar. El cliente 802.11b percibe la información enviada por el cliente 802.11g como ruido.

La intervención de un cliente 802.11b en una red de tipo 802.11g, no se limita solamente a la celda del punto de acceso en la que se encuentra conectado, si se encuentra trabajando en un ambiente con múltiples AP en Roaming, los AP en los que no se encuentra conectado el cliente 802.11b se transmitirán entre sí tramas con la siguiente información:

NON_ERP present: no
Use Protection: yes

La trama anterior les dice que hay un cliente NON_ERP conectado en uno de los AP, sin embargo, al tenerse habilitado Roaming, es posible que éste cliente 802.11b se conecte en alguno de ellos en cualquier momento, por lo cual deben utilizar los mecanismo de seguridad en toda la red inalámbrica, degradando de esta forma el rendimiento de toda la celda. Es por esto que los clientes deben conectarse preferentemente utilizando el estándar 802.11g. Wi-Fi (802.11b / g)

- **802.11n**

IEEE 802.11n es una propuesta de modificación al estándar IEEE 802.11-2007 para mejorar significativamente el rendimiento de la red más allá de los estándares anteriores, tales como 802.11b y 802.11g, con un incremento significativo en la velocidad máxima de transmisión de 54 Mbps a un máximo de 600 Mbps. Actualmente la capa física soporta una velocidad de 300Mbps, con el uso de dos flujos espaciales en un canal de 40 MHz. Dependiendo del entorno, esto puede traducirse en un rendimiento percibido por el usuario de 100Mbps.

El estándar 802.11n fue ratificado por la organización IEEE el 11 de septiembre de 2009.

IEEE 802.11n está construido basándose en estándares previos de la familia 802.11, agregando Multiple-Input Multiple-Output (**MIMO**) y unión de interfaces de red (Channel Bonding), además de agregar tramas a la capa MAC.

MIMO es una tecnología que usa múltiples antenas transmisoras y receptoras para mejorar el desempeño del sistema, permitiendo manejar más información (cuidando la coherencia) que al utilizar una sola antena. Dos beneficios importantes que provee a 802.11n, son la diversidad de antenas y el multiplexado espacial.

La tecnología MIMO depende de señales multi-ruta. Las señales multi-ruta son señales reflejadas que llegan al receptor un tiempo después de que la señal de línea de visión (*line of sight, LOS*) ha sido recibida. En una red no basada en MIMO, como son las redes 802.11a/b/g, las señales multi-ruta son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales multi-rutas para incrementar la habilidad de un receptor de recobrar los mensajes de la señal.

Otra habilidad que provee MIMO es el Multiplexado de División Espacial (SDM). SDM multiplexa espacialmente múltiples flujos de datos independientes, transferidos simultáneamente con un canal espectral de ancho de banda. SDM puede incrementar significativamente el desempeño de la transmisión conforme el número de flujos espaciales es incrementado. Cada flujo espacial requiere una antena discreta tanto en el transmisor como el receptor. Además, la tecnología MIMO requiere una cadena de radio frecuencia separada y un convertidor de analógico a digital para cada antena MIMO lo cual incrementa el coste de implantación comparado con sistemas sin MIMO.

Channel Bonding, también conocido como 40 MHz o unión de interfaces de red, es la segunda tecnología incorporada al estándar 802.11n la cual puede utilizar dos canales separados, que no se solapen, para transmitir datos simultáneamente. La unión de interfaces de red incrementa la cantidad de datos que pueden ser transmitidos. Se utilizan dos bandas adyacentes de 20 MHz cada una, por eso el nombre de 40 MHz. Esto permite doblar la velocidad de la capa física disponible en un solo canal de 20 MHz. (Aunque el desempeño del lado del usuario no será doblado.)

Utilizar conjuntamente una arquitectura MIMO con canales de mayor ancho de banda, ofrece la oportunidad de crear sistemas muy poderosos y rentables para incrementar la velocidad de transmisión de la capa física.

- **802.11ac**

Es una mejora a la norma IEEE 802.11n, se ha desarrollado entre el año 2011 y el 2013, y finalmente aprobada en enero de 2014.

El estándar consiste en mejorar las tasas de transferencia hasta 1 Gbit/s dentro de la banda de 5 GHz, ampliar el ancho de banda hasta 160 MHz (40 MHz en las redes 802.11n), hasta 8 flujos MIMO y modulación de alta densidad (256 QAM).

2.5 Evaluación de prestaciones en redes inalámbricas

A pesar de la creciente actividad en el ámbito de los despliegues multi-salto, sigue siendo necesario establecer, de manera cuantitativa, cuáles son sus posibles beneficios, tanto para los usuarios finales de los sistemas de comunicación, como para los operadores, especialmente teniendo en cuenta el elevado grado de heterogeneidad que también caracterizará las redes inalámbricas.

Desde que surgieron, se han realizado gran cantidad de estudios sobre cualquiera de las tipologías de redes multi-salto que podemos encontrarnos, dada su versatilidad y heterogeneidad. El hecho de que sigan en continua evolución nos muestra que todavía queda mucho por investigar.

De acuerdo con Tanenbaum (2003) [**4**], a medida que evolucionan las redes de comunicación de datos o informáticas, se añaden problemas de tráfico los cuales define como saltos, principalmente se refiere a los errores, la sincronización, la seguridad y la representación de la información. Estos fenómenos afectan en gran magnitud el funcionamiento del enlace inalámbrico. [**5**]

Debido a las múltiples casuísticas y variables que pueden afectar al rendimiento de una red inalámbrica, es necesario llevar a cabo estudios sobre el comportamiento en los diferentes casos. Sin ir más lejos en esta misma universidad se han llevado a cabo proyectos sobre redes inalámbricas, tanto por alumnos [**6**] como por profesores del centro[**7**].

En este proyecto se acomete el estudio del comportamiento en una red multi-salto y la evaluación en sus prestaciones en función del número de saltos inalámbricos que la componen. Pudiendo comprobar y ampliar conclusiones

obtenidas en otros estudios, como en el *Estudio de las variables que influyen para alcanzar el máximo throughput en un trayecto de un sistema inalámbrico multi-salto multicanal* (J. H. Hernán Vásquez, Bolivia 2012) [**8**] donde concluye que:

- *Se alcanza el máximo throughput cuando no se tiene nodos intermedios entre el transmisor y el receptor.*

- *A medida que se aumenta el número de nodos intermedios, el throughput va disminuyendo; aunque se incremente el número de canales.*

2.6 Conclusiones

En este capítulo hemos podido ver una descripción de las diferentes redes inalámbricas que podemos encontrar, junto con sus principales ventajas e inconvenientes. Diferentes tipologías de redes inalámbricas multi-salto, con algunos ejemplos. Y un resumen de los estándares de la familia 802.11 más relevantes para este estudio.

Todo ello nos permite tener una visión clara, de la heterogeneidad de estas redes y la necesidad de realizar estudios sobre sus prestaciones.

En el siguiente capítulo pasamos a detallar el diseño del proyecto realizado.

3. Diseño del proyecto

Para poder llevar a cabo nuestro estudio, se realizó una selección previa de aquellos parámetros que fueran interesantes para poder evaluar las prestaciones en función de una serie de variables, que también fueron definidas previamente.

Una vez seleccionados los parámetros de rendimiento que podían medirse en función de las variables elegidas, se tuvieron en cuenta varias herramientas para poder obtener los valores de esos parámetros de rendimientos en cada prueba.

3.1 Listado de parámetros de rendimiento

Como hemos comentado el objetivo del proyecto es evaluar las prestaciones de routers inalámbricos en diferentes escenarios de red.

Lo primero que debemos hacer es seleccionar todos los valores medibles que podemos utilizar para medir el rendimiento de una red inalámbrica

A continuación detallaremos los indicadores que podemos medir:

- **Throughput:** Se refiere a la tasa promedio de datos o mensajes que han sido transferidos exitosamente y sin errores en la red de un nodo a otro.

- **Estadísticas de retransmisión:** Media de retransmisión de paquetes.

- **Queuing Delay (retardo de cola):** Retardo producido por la acumulación de paquetes en buffers o colas en dispositivos como routers, gateways y brigde.

- **Latencia:** suma de retardos temporales dentro de una red. Un retardo es producido por la demora en la propagación y transmisión de paquetes dentro de la red.

- **Jitter (variación en la latencia):** es la variación en el tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes

para llegar al destino. Este efecto es especialmente molesto en aplicaciones multimedia en Internet como radio por Internet o telefonía IP, ya que provoca que algunos paquetes lleguen demasiado pronto o tarde para poder entregarlos a tiempo. El efecto puede reducirse con un buffer de *jitter*, un buffer de datos, pero a costa de un retardo mayor.

- **Perdida de paquetes UDP:** UDP al ser un protocolo no orientado a conexión, no garantiza la entrega, por lo que se pueden producir pérdidas de paquetes. El porcentaje de pérdidas nos ayuda a evaluar el rendimiento de esa transmisión de paquetes.

3.2 Listado de variables

En el apartado anterior hemos hablado de todos los parámetros que podíamos utilizar para medir prestaciones en la red inalámbrica en el proyecto. Ahora vamos a ver todos aquellas variables que se han modificado para crear los diferentes escenarios y comparativas de pruebas.

- **Saltos inalámbricos:** Se han creado diferentes escenarios jugando con las diferentes posibilidades que ofrecían los 3 routers utilizados. Comenzando con un único router hasta añadir los tres.

- **Potencia de transmisión del router:** La potencia de emisión del dispositivo wifi suele venir definida en *dBm.* A más potencia, con las mismas antenas, la señal alcanzará mayor distancia aunque creará más interferencias. Se han usado las opciones de 6 *dBm* y 18 *dBm.*

- **Canal de emisión:** Como ya se explicó en apartados anteriores, el rango de frecuencia de la banda 2,4GHz se divide en 11 canales, se han usado aquellos que no se interfieran entre ellos, eligiéndose para hacer las pruebas, el canal 2, 6 y 11.

- **Protocolo:** Se ha realizado pruebas con TCP y con UDP.

- **Tamaño de paquete:** Esta opción solo es relevante para las pruebas que se han realizado con UDP. Teniendo en cuenta que el tamaño máximo sin que se divida el paquete es de 1500Bytes (MTU) y debemos descontar las cabeceras de UDP (8B) y de IP (20B), se han realizado las pruebas con los siguientes tamaños: 80B, 800B y 1472B. También se han realizado pruebas con un paquete de 1500B

para provocar fragmentación y comparar con los tamaños de paquete anteriores.

- **Sentido del tráfico:** Se ha hecho una primera batería de pruebas enviando datos en un único sentido y luego se han hecho las mismas pruebas existiendo tráfico de datos en ambos sentidos simultáneamente, lo que en una red inalámbrica es importante porque el tráfico en ambos sentidos compite por el medio.

3.3 Elección de las herramientas a utilizar

Una vez detallado todos los elementos que podemos medir y comparar vamos a describir qué herramientas gratuitas hemos encontrar para poder hacerlo.

Primero exponemos un listado de las que se han tenido en cuenta y las seleccionadas:

- **Iperf** [9]: Permite medir el rendimiento de la red ajustando diferentes parámetros y generando flujos de datos TCP y UDP. Herramienta realizada en C++ multiplataforma, compatible con Unix, Linux y Windows. Permite ejecutarse en modo cliente o servidor, permitiendo generar el flujo en una o ambas direcciones. Puede medir:
    - **Ancho de banda**
    - **Pérdida de paquetes**
    - **Jitter**
    - **Latencia**

- **MRTG**: Herramienta desarrollada en C y Perl, utiliza el protocolo SNMP (Simple Network Management Protocol) para obtener información del tráfico de un dispositivo ya que proporciona la cantidad de bytes que han pasado por ellos distinguiendo entre entrada y salida. Genera un informe en formato HTML con gráficas que proveen una representación visual de la evolución del tráfico a lo largo del tiempo.

- **WIFI Analyzer**: Aplicación móvil que permite monitorizar las redes inalámbricas de nuestro alrededor, permitiendo ver cuáles de ellas se están solapando, en qué canales y también mostrarnos su evolución temporal en cuanto a señal.

- **Nagios**: Es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP,SNMP...). Permite la visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros

- **Wireless Tools de Ubuntu**: Se basa en línea de comandos, lo que permite automatizar mediante scripts.
  Las herramientas que trae son:
  - ***iwconfig***: permite mostrar y editar la configuración de una interfaz de red inalámbrica
  - ***.iwspy:*** permite monitorizar una lista de nodos inalámbricos y registrar la calidad del enlace de cada uno de ellos.
  - ***Iwpriv:*** permite configurar parámetros opcionales de una interfaz de red inalámbrica.

- **Wireshark / Tshark:** antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica y muchas opciones de organización y filtrado de información. También incluye una versión basada en texto llamada tshark.

- **Tcpdump:** es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar a tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado. funciona en la mayoría de los sistemas operativos UNIX: Linux, Solaris, BSD, Mac OS X, HP-UX y AIX entre otros. En esos sistemas, tcpdump hace uso de la biblioteca libpcap para capturar los paquetes que circulan por la red.

Finalmente se ha usado ***iperf***, ya que cumplía todos los requisitos necesarios, permitiendo generar tráfico UDP y TCP, parametrizando aquellos valores necesarios de la transmisión relevantes para las pruebas, y mostrando

el resultado de los parámetros de rendimiento que se querían evaluar, de forma sencilla.

Para obtener la latencia, se ha usado ***ping***.

3.4 Descripción de la infraestructura

El modelo de router utilizado es: **LINKSYS WRT54GL** que permite trabajar con los siguientes estándares: IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b, los dos últimos son los que aplican a este proyecto.

Figura 6: Imagen del router Linksys WRT54GL

Se ha trabajado con un ordenador de mesa sin tarjeta inalámbrica y un portátil con wifi, ambos con el sistema operativo Ubuntu.

El escenario ha sido un laboratorio de la universidad Carlos III, realizando todas las pruebas en el interior de la sala.

3.5 Conclusiones: Selección de herramientas

Una vez seleccionados todos los parámetros de rendimiento relevantes para nuestro estudio y las variables que podían modificarse en las pruebas se seleccionó la herramienta ***iperf***, ya que cumplía todos los requisitos necesarios, permitiendo generar tráfico UDP y TCP, parametrizando aquellos valores necesarios de la transmisión, y mostrando el resultado de los parámetros de rendimiento que se querían evaluar, de forma sencilla.

Para obtener la latencia, se ha usado ***ping***.

Con todas las herramientas y parámetros seleccionados se realizaron una batería de diversas pruebas cuyos resultados se detallan en el capítulo siguiente.

Para poder realizar las modificaciones de los parámetros en los routers de una manera sencilla y automática se han creado una serie de scripts que se detallan en el capítulo 4 y pueden encontrarse en el apéndice. También se han creado scripts para automatizar la recogida de la salida de iperf.

4. Automatización

Para llevar a cabo las pruebas de una manera más ágil y automática se han realizado algunos scripts que han facilitado la recogida de información de las pruebas y los cambios de configuración de los routers. Los scripts pueden verse en el apéndice 8.2 de este proyecto.

4.1 Cambio de parámetros en los routers

Se ha realizado un script cambiar_param.sh que en base a un fichero de configuración donde se han incluido las IPs de los routers a editar, y unas serie de opciones se modificaban los valores de potencia de señal, el canal y el estándar en cada router.

Para poder ejecutar este script de forma automática, dado que requiere una conexión a cada router, se han configurado claves ssh en cada uno, para que no solicitara password en la conexión.

4.2 Recogida datos latencia

Para obtener la latencia de la conexión se ha utilizado el comando *ping.* Se ha creado un script que permite recoger la salida de este comando y almacenarla en formato csv junto con la configuración que tiene cada router en ese momento para poder tratar la información con mayor facilidad.

4.3 Recogida datos pruebas TCP y UDP

Para obtener la mayor parte de la información que se ha evaluado en este proyecto se ha usado el comando *iperf*. Se ha creado un script que permite recoger la salida de este comando y almacenarla en formato csv junto con la configuración que tiene cada router en ese momento para poder tratar la información con mayor facilidad.

Una vez elegidas todas las herramientas a utilizar, los escenarios a evaluar y realizada la automatización se pudo continuar con las fase de pruebas que se describen el siguiente capítulo.

5. Pruebas

Una vez elegidas las herramientas con las que trabajar y hecha la selección de parámetros, se definen los diferentes escenarios y el listado de pruebas que se realizaran en ellos.

5.1 Escenarios

Se ha trabajado con 4 escenarios diferentes, en función del número de saltos inalámbricos formado por los routers Lynksys disponibles, la distancia entre estos saltos, y el modo del enlace inalámbrico, pudiendo ser en modo infraestructura o modo ad hoc. Todas las topologías tienen una máscara de red /24.

1 ROUTER

Figura 7: Imagen conexión un único router como AP

Como se representa en la *Figura 7, s*e conecta el PC por cable al router, ya que no dispone de tarjeta inalámbrica y el portátil por WI-FI al mismo router.

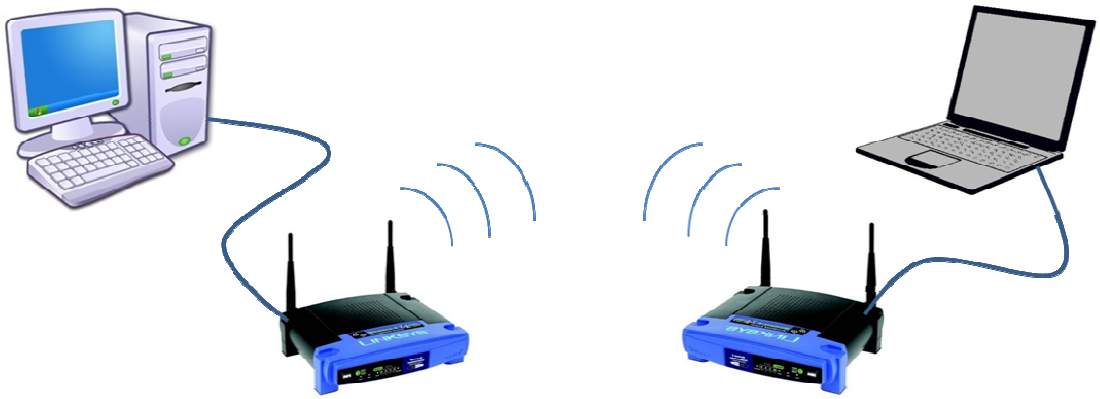
El router se ha configurado como Punto de Acceso (AP) y el portátil se conecta a éste en modo cliente, de forma equivalente a como nos conectaríamos en nuestra casa. Sería una conexión de red de infraestructura. En la *Figura 8* podemos ver su topología de red.

Figura 8: Topología de red conexión un único router como AP

2 ROUTERS

Una primera idea era haber conectado únicamente por cable el PC de mesa al primer router y el portátil de forma inalámbrica, pero después de diferentes pruebas se ha visto que, aunque no debería ser así, no eran compatibles los modos ad hoc del router y del portátil. Por lo que el segundo escenario, se ha creado con 2 routers con conexión inalámbrica entre sí, y conectados cada uno a su respectivo servidor (*ver Figura 9)*.

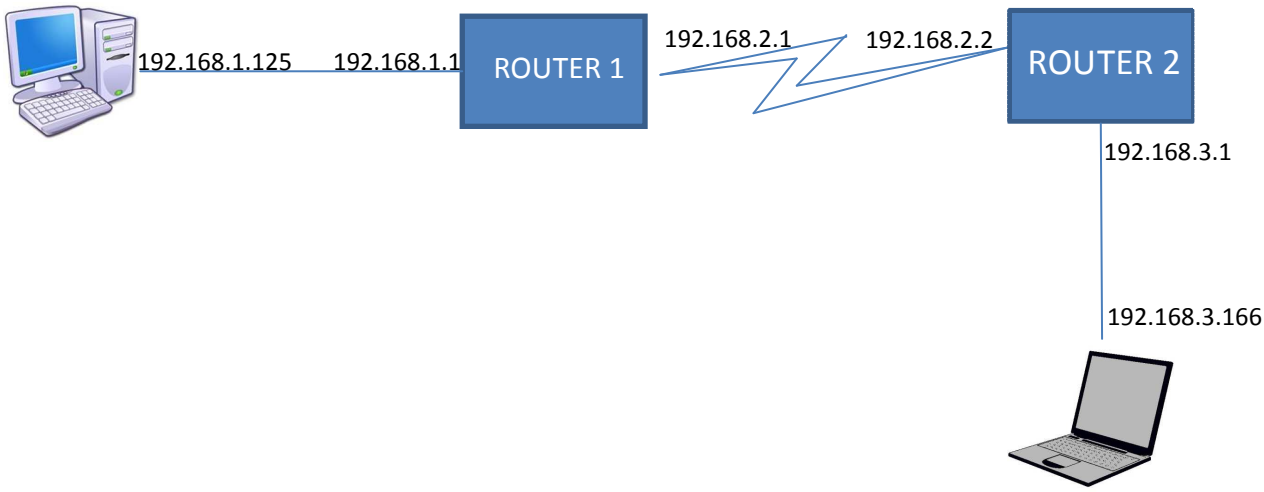
Figura 9: Imagen conexión dos routers modo ad hoc



Para realizar esta conexión se han configurado ambos routers, al contrario que en el caso anterior que era modo infraestructura, en modo ad hoc. Es necesario cambiar la IP de la interfaz LAN del router 2 para que no coincida con la IP del router 1, ya que todos los routers traen la misma IP por defecto. Se crea un *ssid* único y se configura en ambos routers, ya que deben coincidir para poder reconocerse (y participar así en la misma red ad hoc).

El dibujo de red puede verse en la *Figura 10.*

Figura 10: Topología de red conexión dos routers modo Ad Hoc



3 ROUTERS

El último escenario en el que se ha trabajado es con tres routers, añadiendo un nuevo salto inalámbrico (*ver Figura 11)*. De este mismo escenario se han realizado pruebas con dos vertientes, una teniendo los tres routers sobre la misma mesa del laboratorio y otra separando el router intermedio todo lo que permitía la sala, aproximadamente 8 metros .

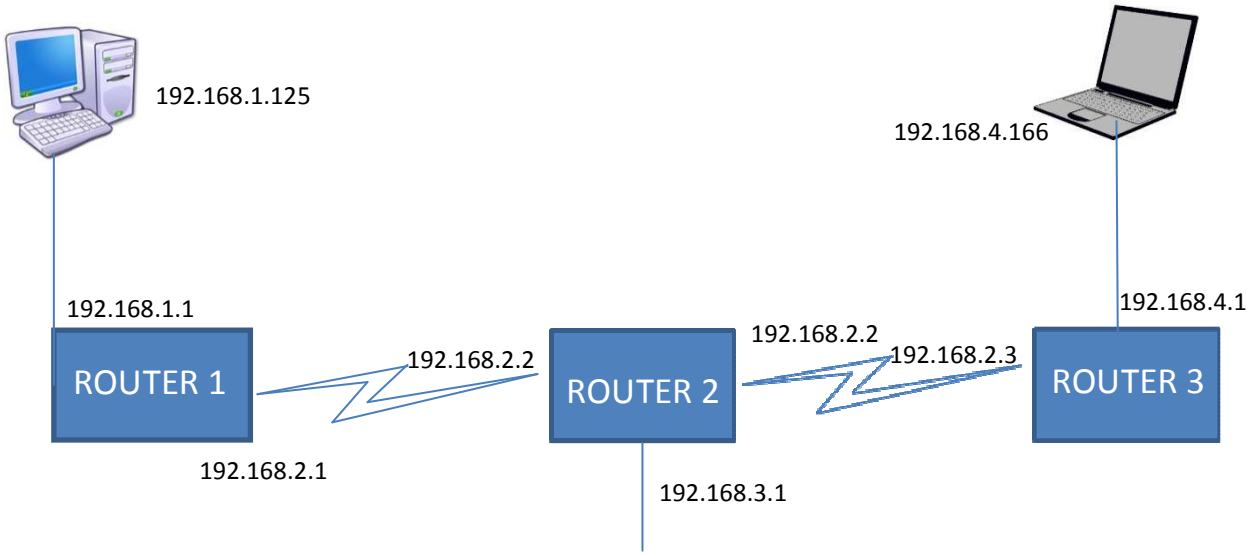
Figura 11: Imagen conexión tres routers modo Ad Hoc

Para añadir el Router 3 a la ecuación no es necesario editar los ficheros de configuración de red del Router 1. En el Router 2 como ya le habíamos dado una IP de una red distinta diferente a la LAN del Router 1, la mantenemos. Y añadimos una nueva ruta en el fichero /etc/config/network para poder encaminar los paquetes a la red del tercer router añadido (*ver topología de red en la Figura 12)*.

En el Router 3 modificamos la IP que trae por defecto el router dándole a la LAN una IP de una nueva red. Al igual que en los otros routers, se añade la interfaz wifi y la ruta de encaminamiento.

Además de las configuraciones nombradas, para poder trabajar en este escenario y que los nodos fueran visibles ha sido necesario desactivar el firewall de cada router.

Figura 12: Topología de red conexión tres routers modo Ad Hoc



5.2 Pruebas

A continuación se detallan las pruebas que se han realizado en los diferentes escenarios:

- Pruebas de latencia.
- Pruebas con dos protocolos de transmisión: TCP y UDP
- Pruebas con tráfico unidireccional y bidireccional.
- Pruebas en diferentes canales (channel 2, channel 6 y channel 11).
- Pruebas con diferentes potencias de señal (6dBm y 18 dBm).

Con UDP además se han realizado:

- Pruebas con diferente tamaño de buffer (80B, 800B, 1472B y 1500B).
- Pruebas con diferentes flujos de tráfico generados.

Para la realización de estas pruebas se han usado los comandos de ping e iperf. Se han desarrollado unos scripts para poder recoger la salida de las pruebas de forma más automática y para poder modificar las configuraciones de los routers sin necesidad de editar los ficheros de configuración manualmente. Buscando una mayor automatización del proceso evitando potenciales fallos derivados de la manualidad y aumentando la posibilidad de control del mismo.

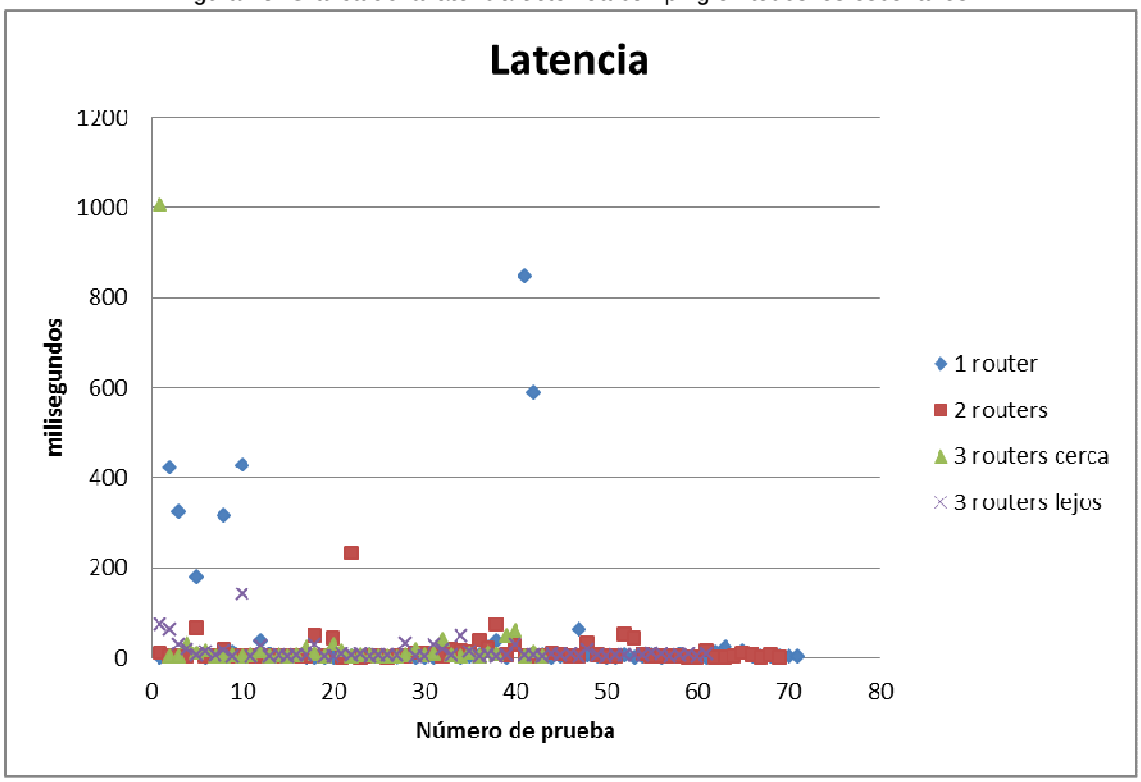
5.3 Resultados

En este apartado vamos a evaluar los resultados obtenidos en las pruebas nombradas en el punto anterior mediante gráficos ya que es una manera más visual de presentar los resultados y extraer conclusiones.

5.3.1. Latencia

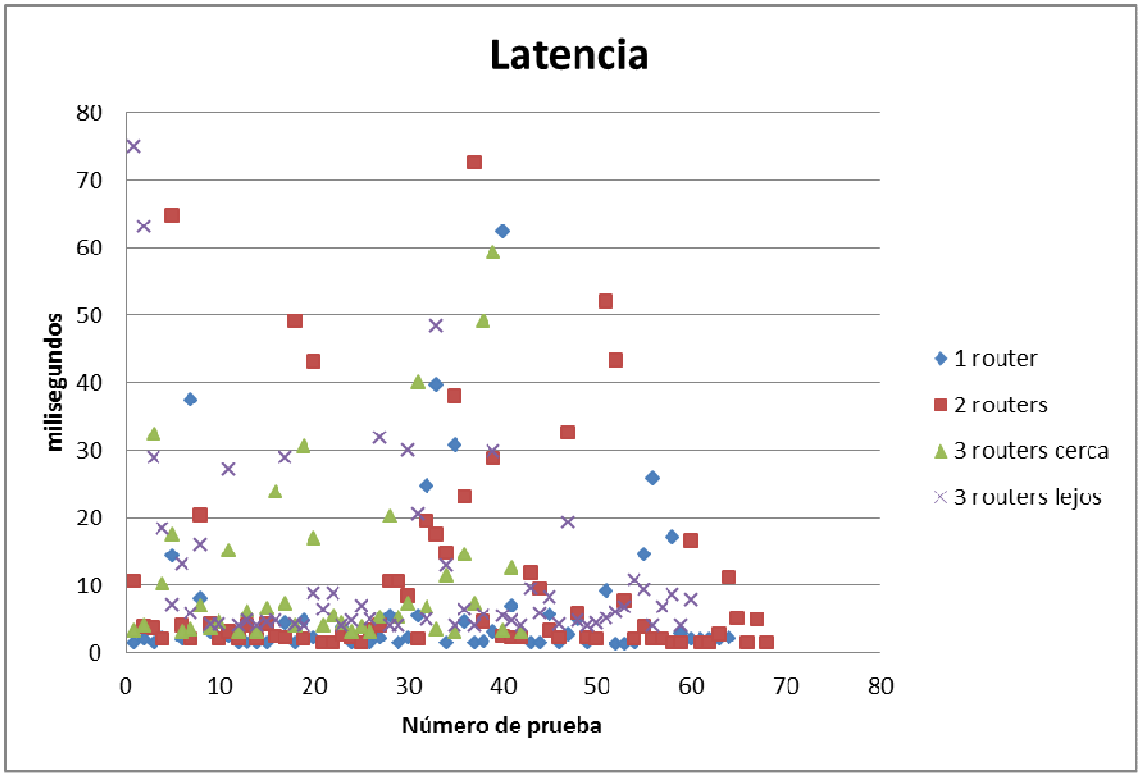
En este primer gráfico (*ver Figura 13)* se muestra la latencia obtenida en los 4 escenarios que se han evaluado, los resultados se han obtenido en el canal 11 con las diferentes potencias de transmisión (6 y 18dBm) y con diferente modo 802.11 (802.11b, 802.11g y 802.11gb), aunque se representan en una única gráfica ya que no se han visto diferencias concluyentes entre los resultados de cada modo:

Figura 13: Gráfica de la latencia obtenida con ping en todos los escenarios



Como podemos observar hay algunas pruebas que han dado una latencia excesiva, vamos a representar un segundo gráfico sin estos picos para poder tener una visión más clara sin distorsión:

Figura 14: Gráfica de la latencia obtenida con ping en todos los escenarios, eliminando puntos máximos.

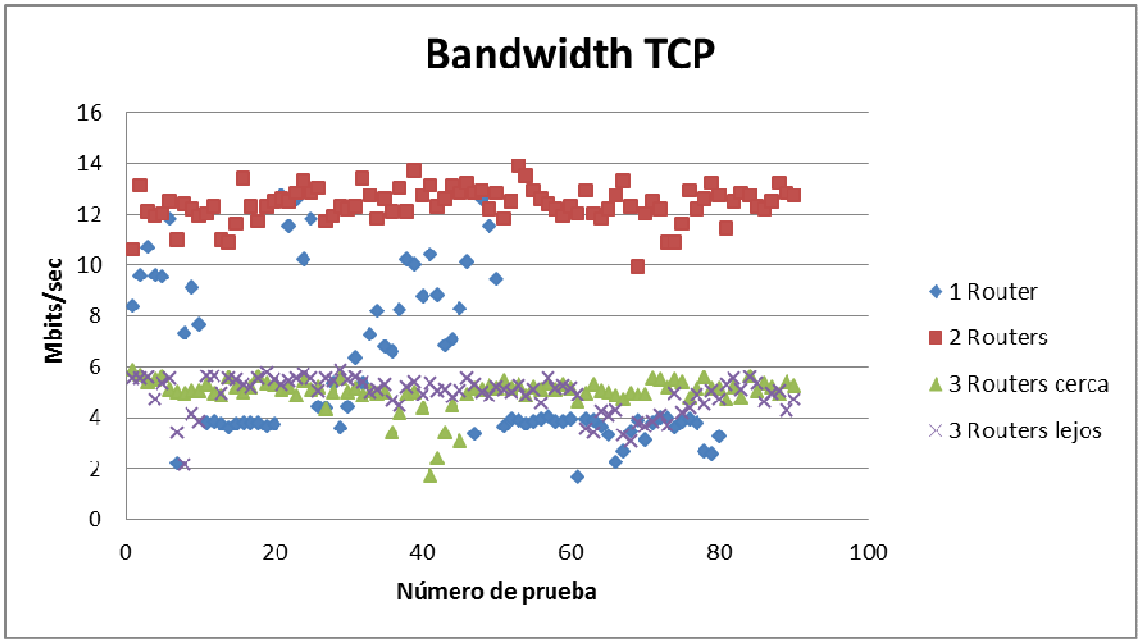


Puede observarse que no hay una diferencia clara entre las latencias de un escenario y otro. El muestreo de la latencia se ha obtenido mediante el comando ping, lo que podría explicar que no haya una diferencia importante, ya que el tamaño del paquete enviado es pequeño (32 bytes), generando poca carga en la red.

5.3.2. Throughput en TCP

En el siguiente gráfico vamos a evaluar el *throughput* obtenido en las pruebas realizadas con TCP:

Figura 15: Bandwidth TCP en todos los escenarios



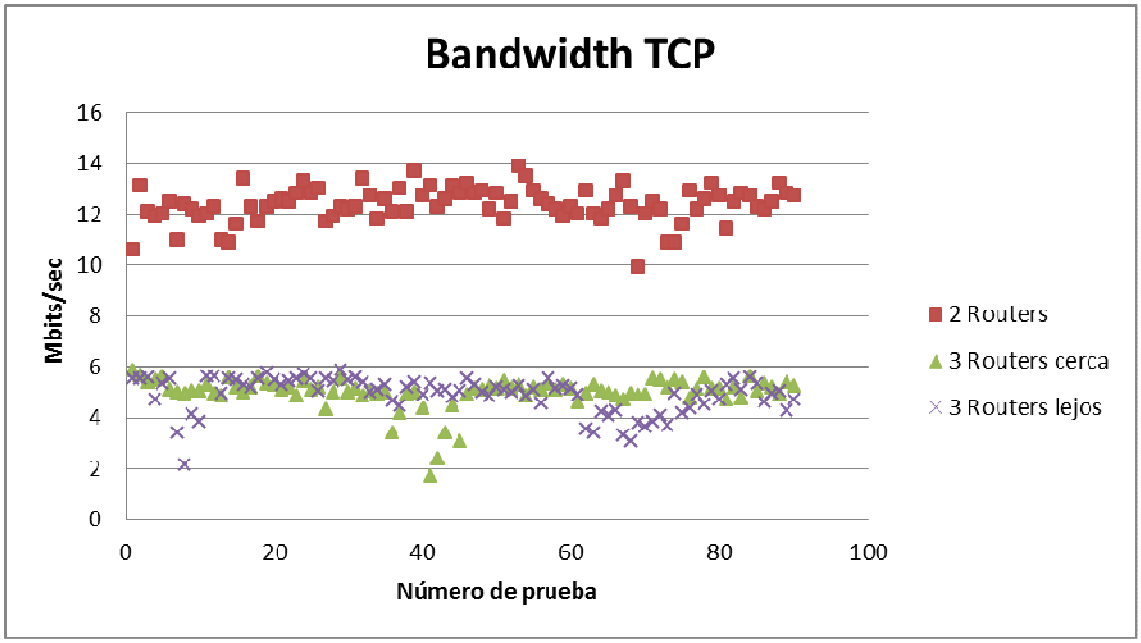
Podemos ver que el mejor ancho de banda real obtenido es en la conexión con dos routers conectados en modo ad hoc (*ver Figura 15 y Figura 16)*.

Estos datos se han obtenido generando tráfico en un único sentido, se han tomado muestras en diferentes canales WI-FI y con diferente potencia de transmisión. Pero como puede verse en la gráfica (*ver Figura 15)*, cada escenario se mantiene estable y la única diferencia es entre los diferentes saltos inalámbricos.

En línea con otros estudios [**8**] hemos verificado que el throughput va disminuyendo al aumentar el número de nodos inalámbricos.

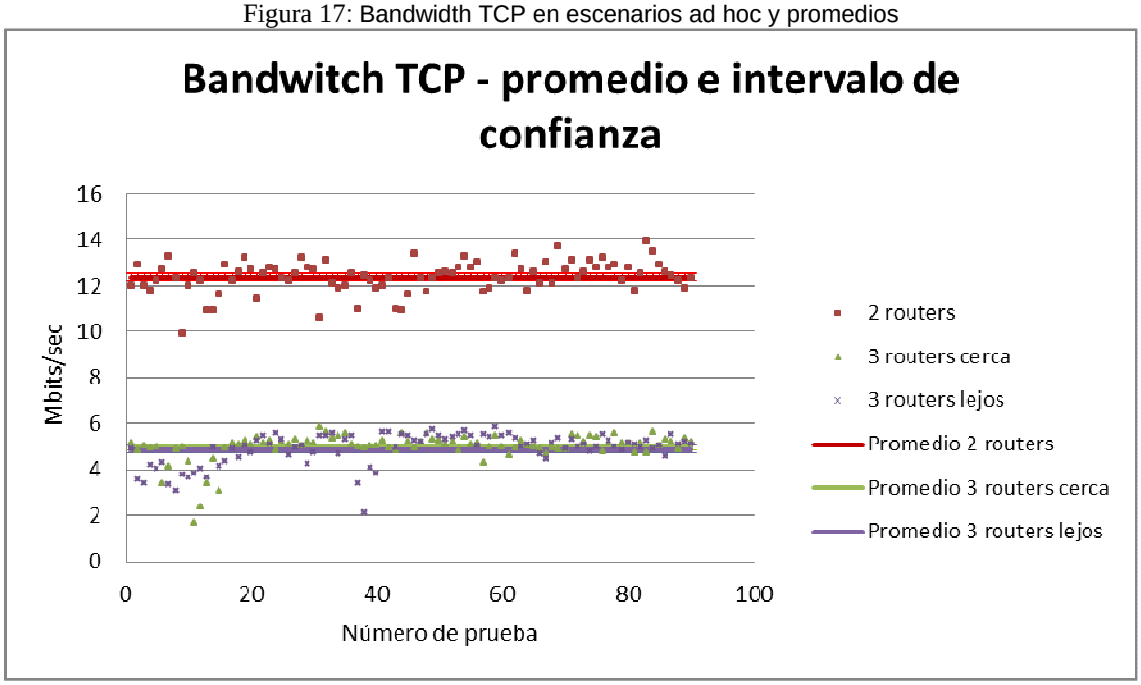
Sacando de la ecuación la prueba con un único router a haber sido realizada con un modo de infraestructura en vez de en modo ad hoc (*ver Figura 16*). Podemos observar que en este caso esas conclusiones son aplicables, encontrandonos una degradación del throughput al añadir el tercer router.

Figura 16: Bandwidth TCP en escenarios ad hoc



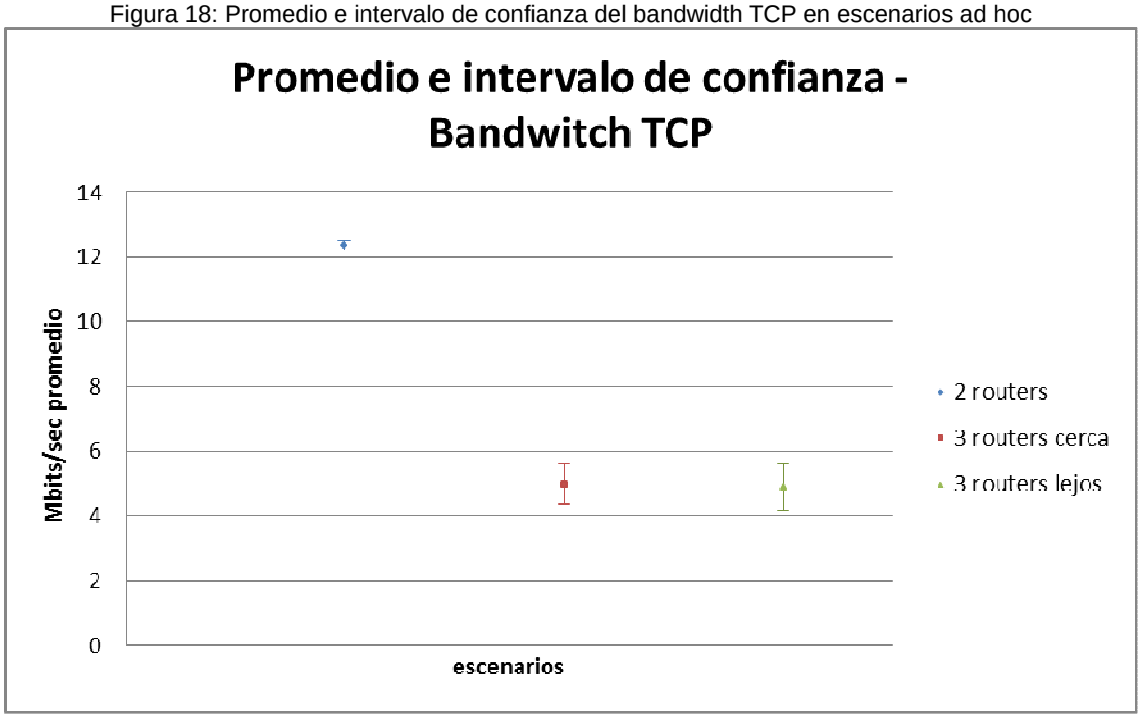
Finalmente representamos la misma gráfica con los promedios de cada escenario y sus intervalos de confianza (*ver Figura 18 y Figura 17*), donde podemos ver que el promedio de los escenarios con tres routers es muy similar.

Figura 17: Bandwidth TCP en escenarios ad hoc y promedios



Como en la gráfica anterior no se aprecia adecuadamente el intervalo de confianza del promedio, representamos el promedio como un único punto junto con el intervalo de confianza en una gráfica a parte (*ver Figura 18*).

Figura 18: Promedio e intervalo de confianza del bandwidth TCP en escenarios ad hoc



5.3.3. Throughput en TCP con diferente potencia de transmisión

Dado que los muestreos de las gráficas anteriores se han obtenido en diferentes canales (*ver Figura 21, Figura 22 y Figura 23)* y con diferente potencia de transmisión (*ver Figura 19 y Figura 20)*, separamos en gráficas diferentes según la variable para evaluar si se han obtenido mejores resultados en alguno de los casos. Comparamos solo con los resultados de los escenarios en modo ad hoc.

Figura 19: Bandwidth TCP en escenarios ad hoc con tx de 6dBm

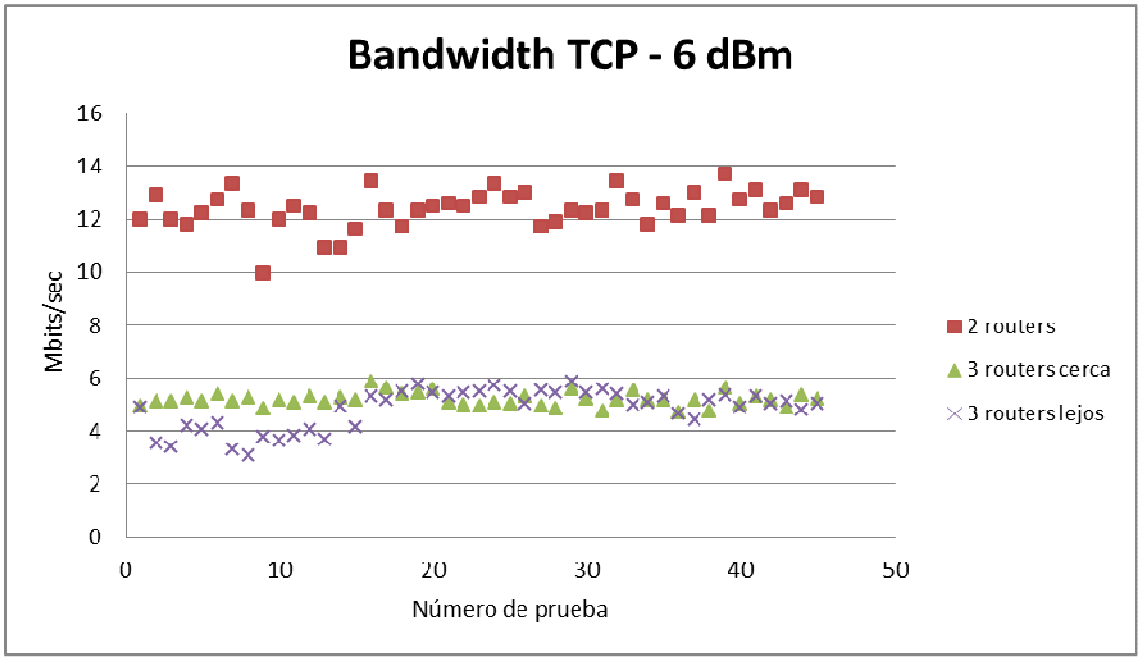
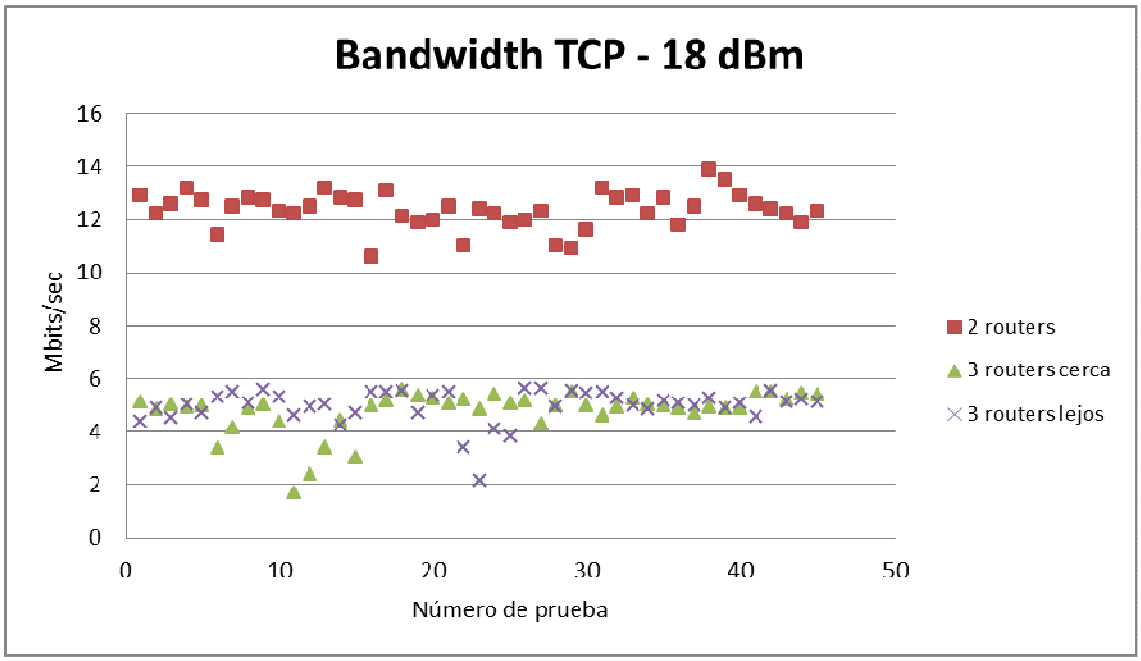


Figura 20: Bandwidth TCP en escenarios ad hoc con tx de 18dBm



5.3.4. Throughput en TCP en diferentes canales de frecuencia

Realizamos la misma comparativa que el cápitulo anterior para la potencia de transmisión, con los canales de frecuencia utilizados.

Figura 21: Bandwidth TCP en escenarios ad hoc en el canal 2

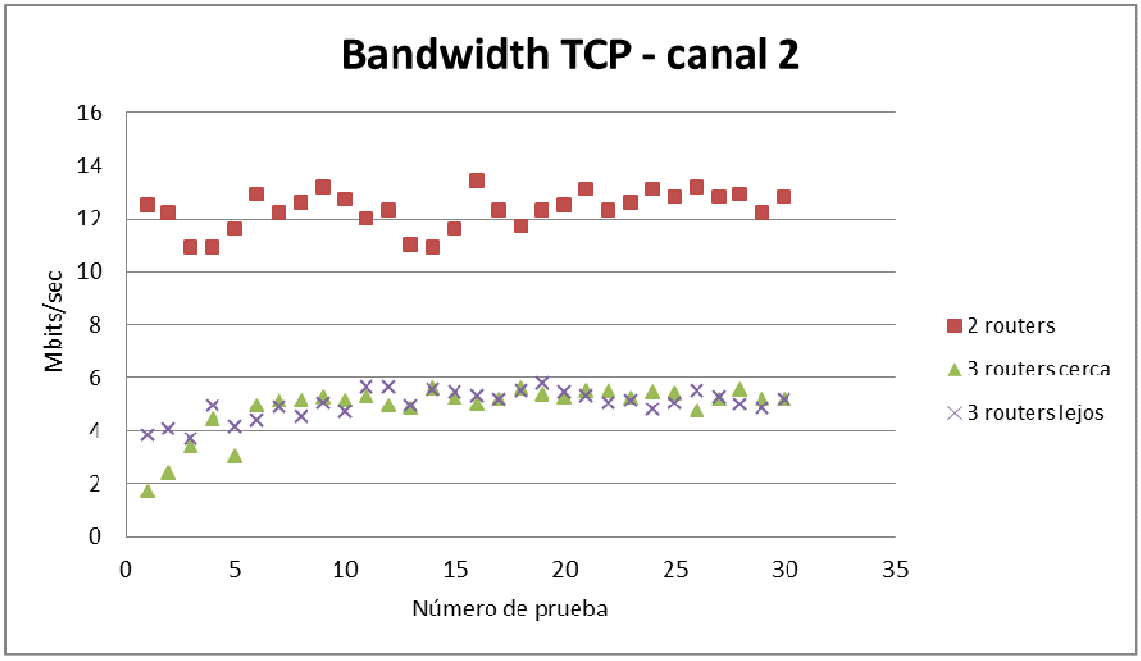


Figura 22: Bandwitch TCP en escenarios ad hoc en el canal 6

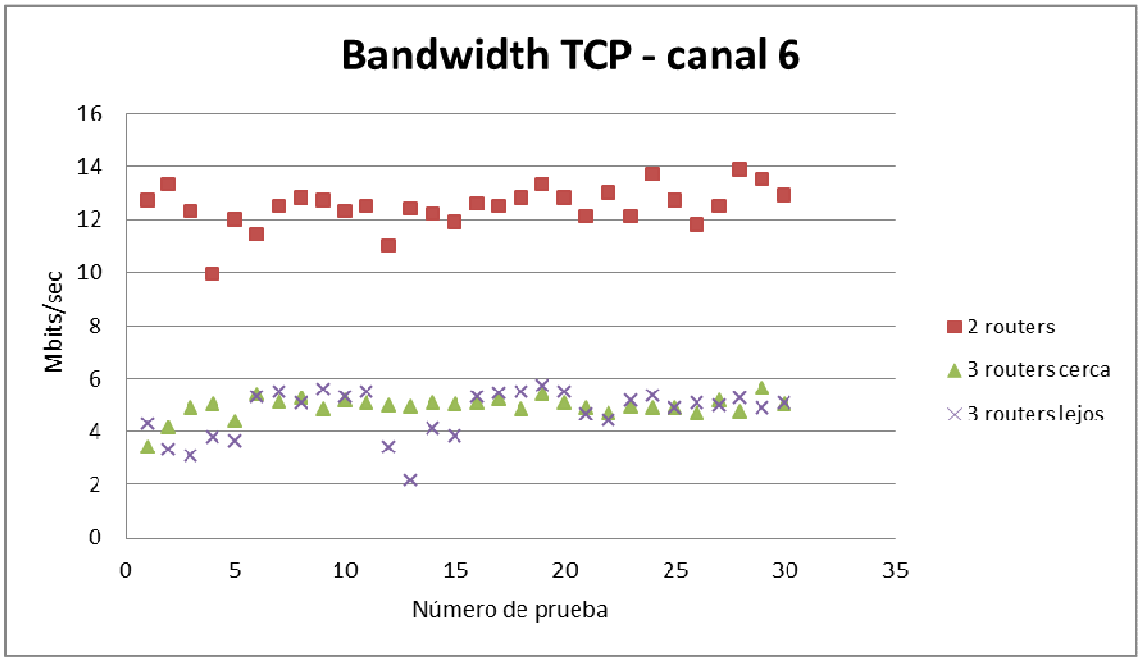
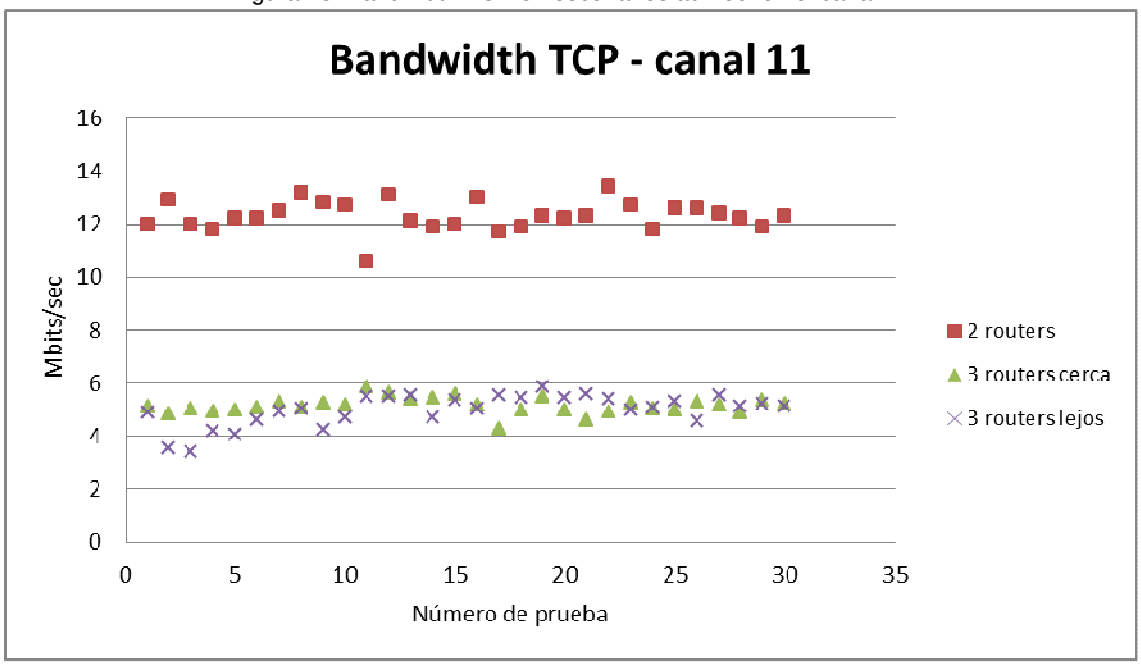


Figura 23: Bandwidth TCP en escenarios ad hoc en el canal 11



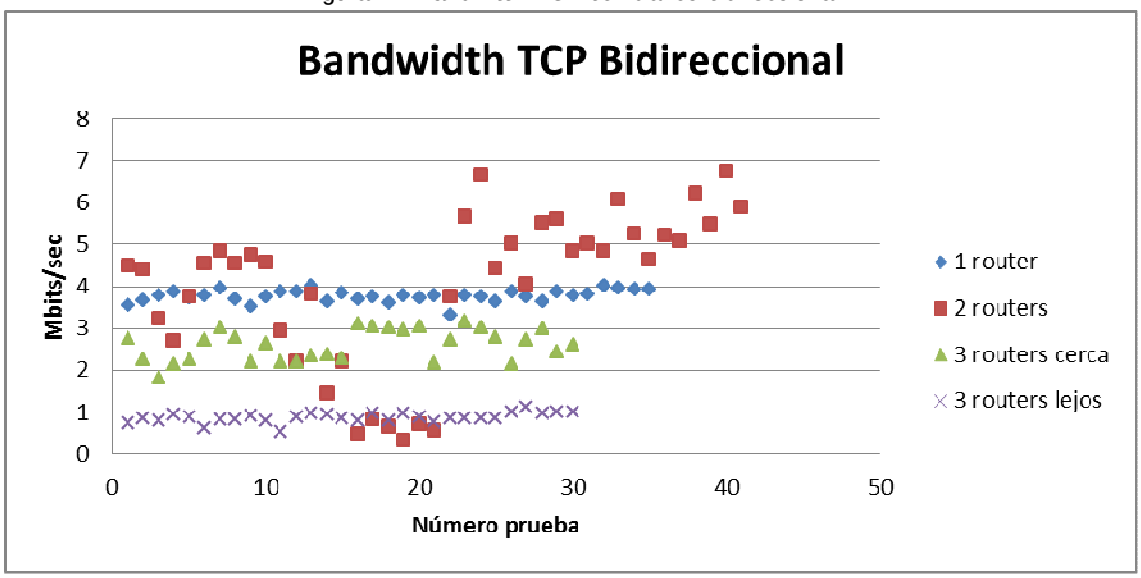
Si comparamos los resultados obtenidos entre las diferentes gráficas en función del canal, no hay una diferencia destacable entre los datos obtenidos en una canal de frecuencia y otro.

5.3.5. Throughput en TCP con tráfico bidireccional

Se ha realizado un segundo muestreo provocando el mismo tráfico en el sentido inverso, es decir, teniendo tráfico en ambos sentidos. Este tráfico se ha generado ejecutando otro comando iperf en sentido contrario con los mismos parámetros. Las muestras recogidas, son del resultado del iperf en el sentido original. A pesar de que en TCP siempre existe tráfico bidireccional, ya que se envía un ACK cada dos segmentos de datos recibidos, son menos paquetes y de un tamaño menor del generado en esta prueba, por lo que al tener dos flujos que compiten por igual con el medio inalámbrico, en throughput se reduce a la mitad, siendo inferior en algunos casos, por lo que se está teniendo una penalización por esa compartición del medio (*ver Figura 24)*.

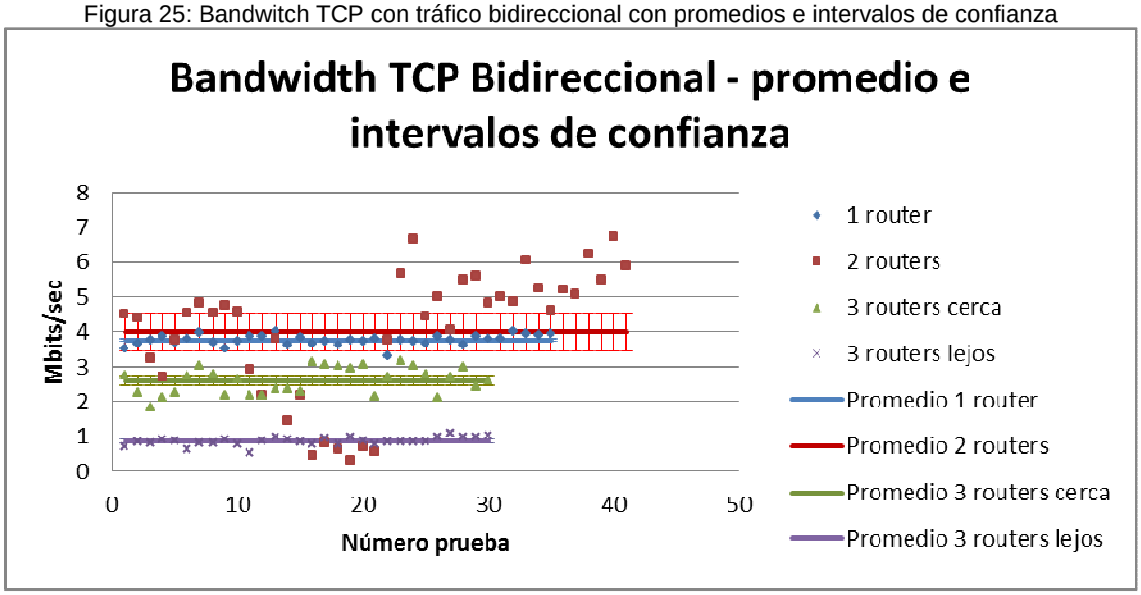
Como se ha demostrado en el punto 4.3.4, no se ha visto diferencias entre los muestreos según los diferentes canales, en las pruebas que afectan a la siguiente gráfica se han tomado los datos en único canal, el 11.

Figura 24: Bandwitch TCP con tráfico bidireccional



Al igual que ya vimos en la *Figura 17*, representamos en la *Figura 25*, los mismos datos que en la *Figura 24* añadiendo los promedios e intervalos de confianza.

Figura 25: Bandwitch TCP con tráfico bidireccional con promedios e intervalos de confianza

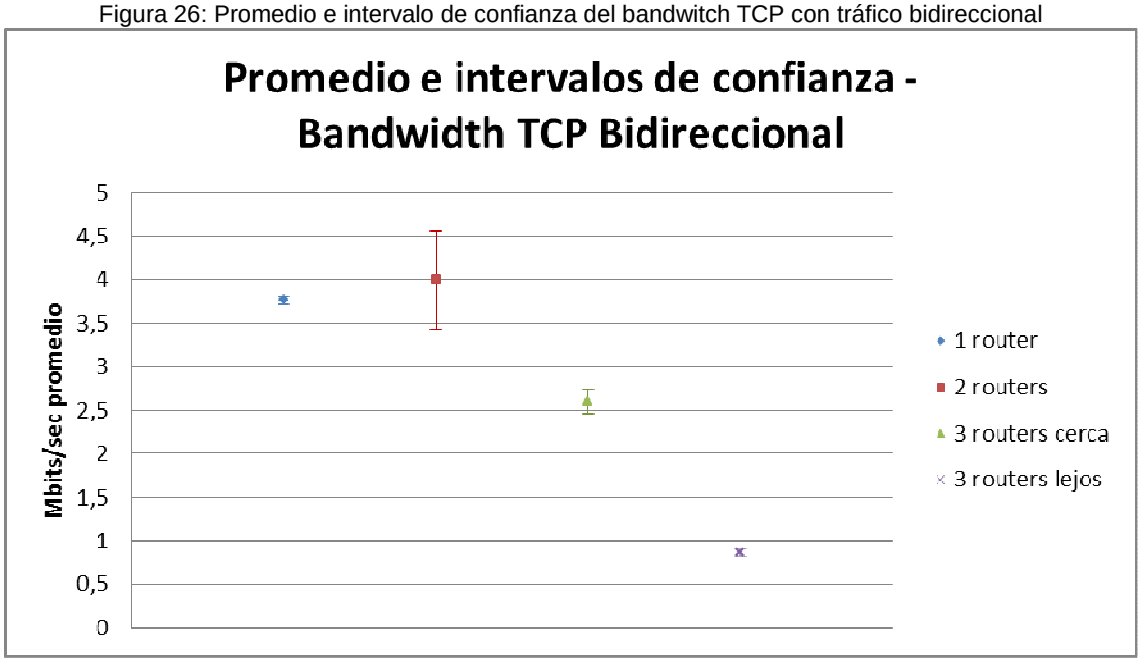


También vemos en la siguiente gráfica (
Figura **26***),* representado de forma individual los promedios y sus intervalos de confianza.

Podemos ver que con un salto inalámbrico (escenario con 2 routers) el throughput total del caso de tráfico de datos bidireccional (4 Mbit/s + 4 Mbit/s= 8 Mbit/s) está lejos del total con tráfico de datos unidireccional (12,05 Mbit/s, *Figura 17*). Con 3 routers cerca, el throughput total (2,5 Mbit/s + 2,5 Mbit/s = 5

Mbit/s) es similar al total del caso de tráfico de datos unidireccional (5 Mbit/s, *Figura 17*), probablemente porque en este caso, incluso con tráfico de datos unidireccional, al tener varios routers intentando enviar a la vez, tenemos una penalización por los asentimientos en sentido contrario y la competencia entre los routers por el medio. En el caso de tráfico bidireccional con 3 routers, uno de ellos lejos, las prestaciones son todavía peores.

Figura 26: Promedio e intervalo de confianza del bandwitch TCP con tráfico bidireccional



En las gráficas anteriores se ha detallado los resultados más relevantes respecto a las pruebas ejecutadas con TCP, a continuación se verán los resultados de las pruebas con UDP.

5.3.6. Pérdida paquetes UDP

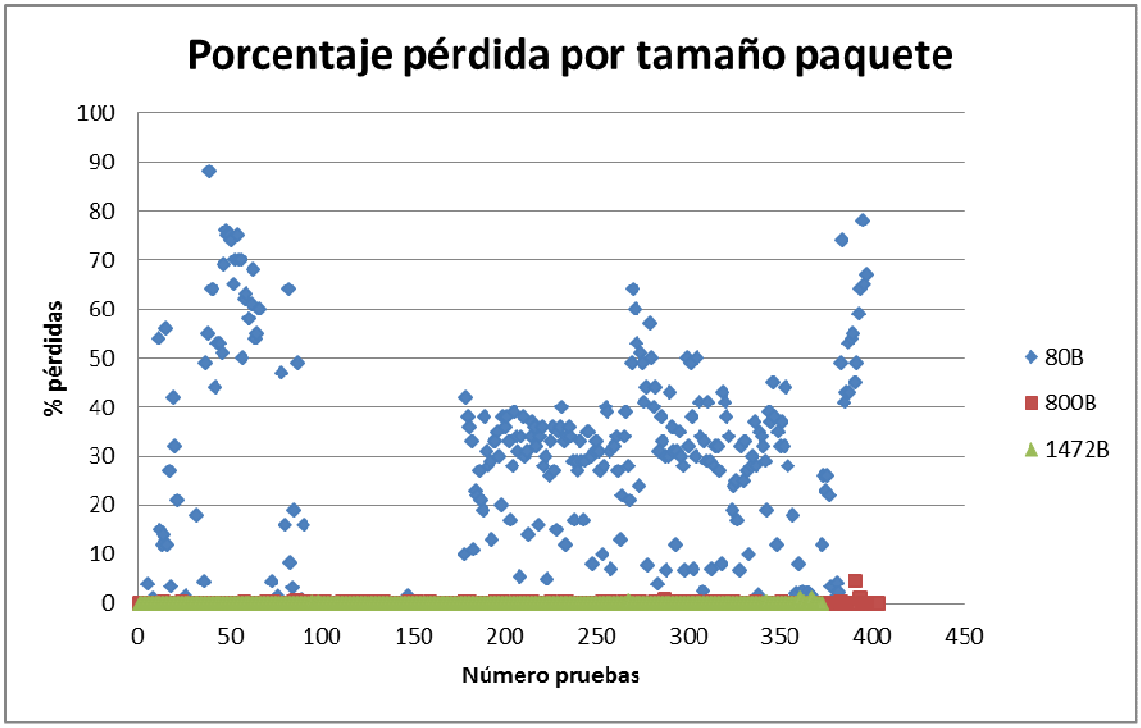
En UDP se han tratado otras variables que permiten evaluar el rendimiento, como es la perdida de paquetes, esto no es posible verlo con TCP ya que no se producen perdidas, si no que se reenvían los paquetes en caso de que se produzcan. Se ha variado el tamaño de datos enviados ya que UDP pone en cada datagrama exactamente los datos de una escritura para su envío, de esta manera se ha controlado el tamaño los paquetes en la red. Como en Ethernet la MTU es de 1500 bytes (y para el modo infraestructura, la MTU de la interfaz wireless también es 1500B), se ha trabajado con ese máximo de paquete para que no se fragmentará y perdieramos el control del tamaño real del paquete que se iba a poner en la red.

Para obtener es tamaño máximo de paquete, debemos descontar el tamaño de la cabecera IP (20B) y de la cabecera UDP (8B), por lo que el tamaño de paquete que debemos generar es, 1500 – 20 – 8 = 1472B.

Tomando como máximo el tamaño de paquete de 1472 bytes, se han realizado las pruebas con los siguientes tamaños: 80B, 800B y 1472B, de esta manera se han evaluado los resultados con un tamaño de paquete muy pequeño, un intermedio y el máximo. Como throughput generado por el cliente se ha mantenido el defecto de iperf para UDP, siendo 1Mbps.

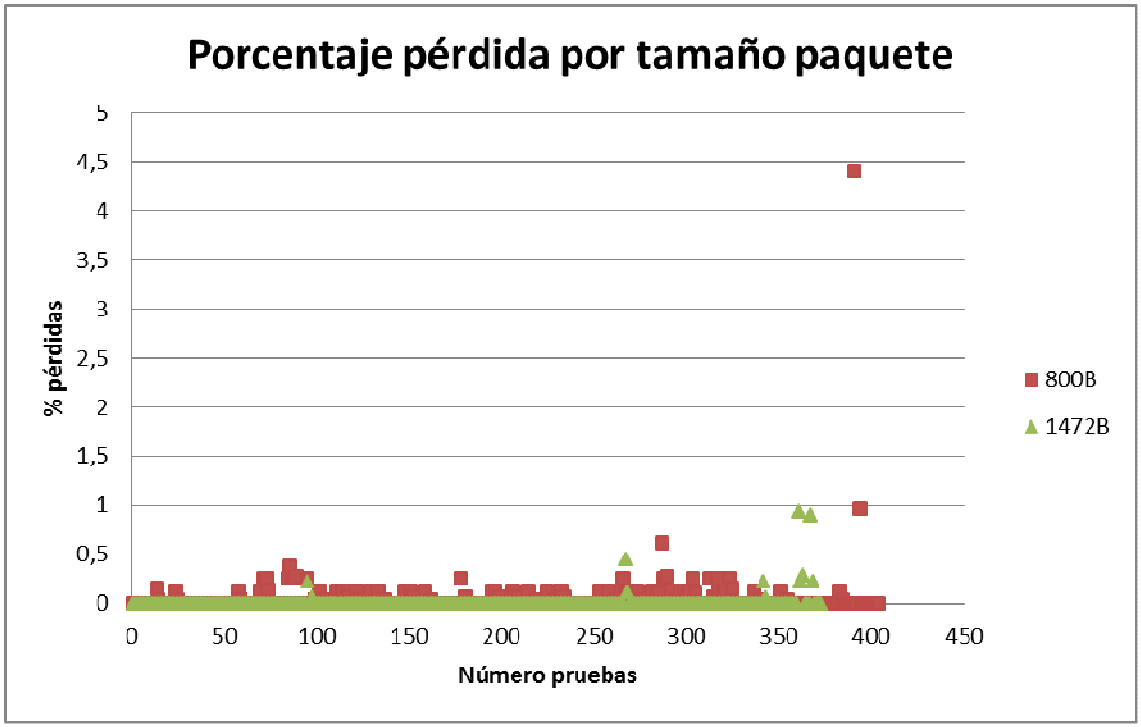
Para formar esta gráfica (*ver Figura 27)* se han usado todos las muestras, incluidos los diferentes escenarios, con ello lo que se quiere representar es que en todos los caso hay una envidencia clara, en la que se demuestra que con un tamaño pequeño de paquete las perdidas de paquete se incrementa de forma grande. Esto es razonable, ya que cada paquete compite por el medio inalámbrico, al enviar el mismo número de bit/s pero repartido en muchos más paquetes la probabilidad de pérdida es mucho mayor.

Figura 27: Porcentaje pérdida de paquetes UDP por tamaño de paquete enviado



Si sacamos del gráfico el tamaño de paquete inferior (*ver Figura 28)*, podemos comparar entre un tamaño de paquete de 800B y el máximo que permite la MTU sin llegar a fragmentar.

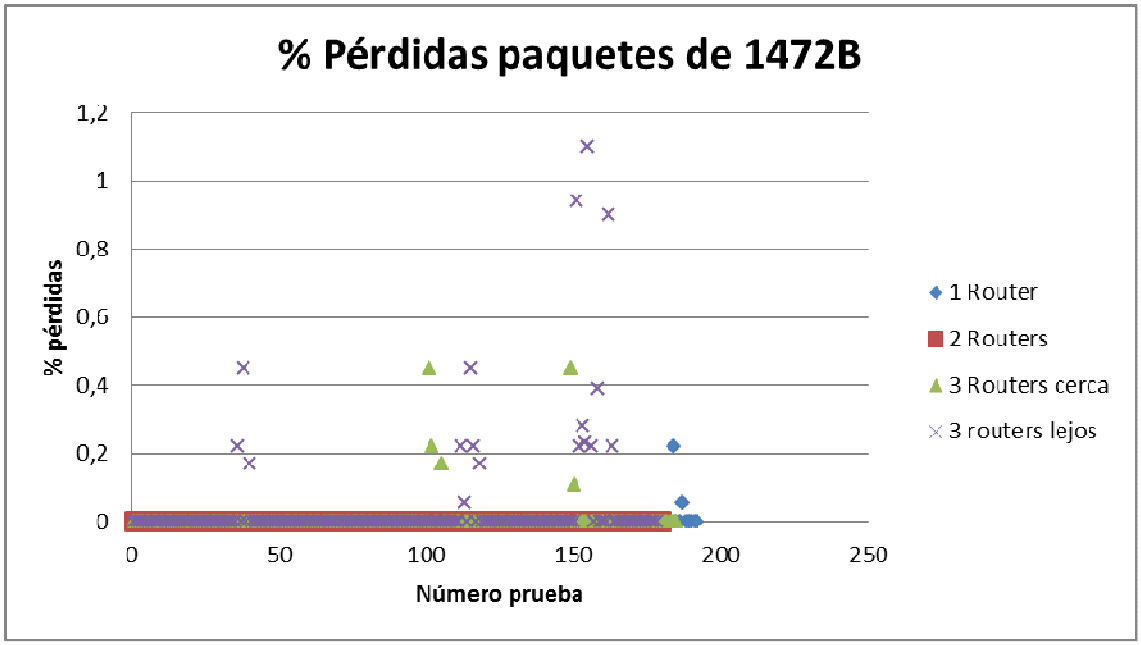
Figura 28: Porcentaje pérdida de paquetes UDP, comparativa paquete medio y máximo



Aunque en ambos casos se producen pérdidas de paquetes, no superan el 1% del total, al contrario de lo sucedido con un tamaño de paquete mínimo que en algunos casos llega a perder más de 80%.

Si tomamos como ideal el tamaño de paquete de 1472B y comparamos entre las diferentes tipologías de saltos inalámbricos en las que se ha trabajado, obtenemos el gráfico representado en la *Figura 29*.

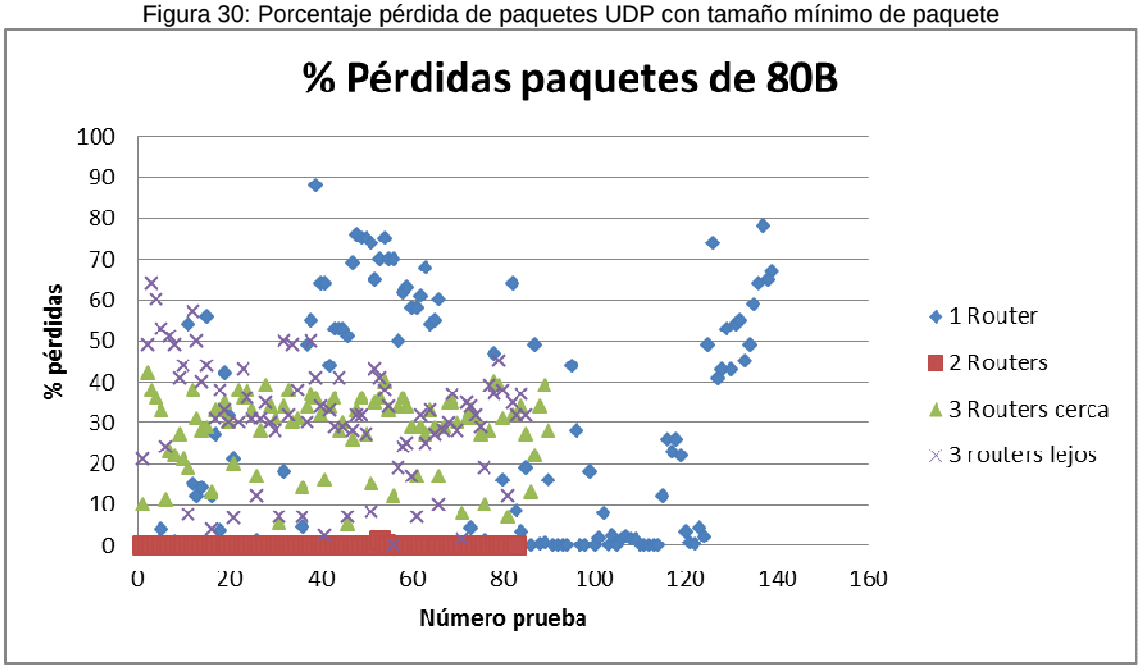
Figura 29: Porcentaje pérdida de paquetes UDP con tamaño máximo de paquete



Aunque la pérdida de paquete es mínima al enviarse el tamaño máximo de paquete posible sin fragmentación, empiezan a verse pérdidas al incrementar el número de saltos inalámbricos, siendo peores los resultados cuando hay más distancia entre ellos.

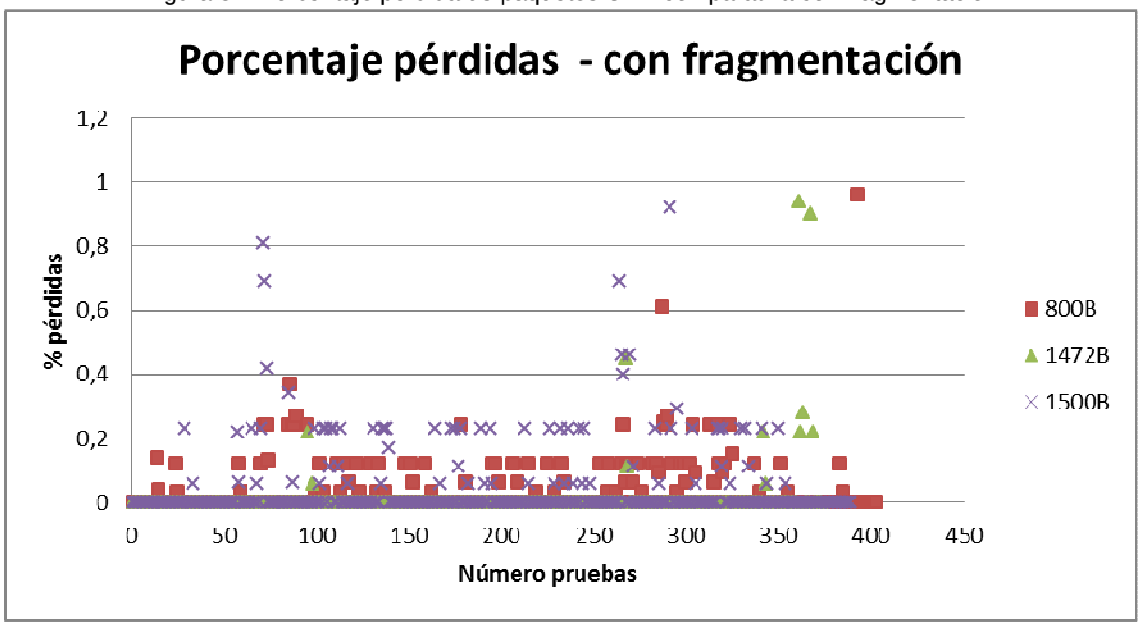
Si por el contrario evaluamos la peor situación, es decir, el muestreo con el tamaño de paquete más pequeño, solo en el escenario más óptimo (un único salto inalámbrico en modo ad hoc), obtenemos unos resultados aceptables (*ver Figura 30*).

Figura 30: Porcentaje pérdida de paquetes UDP con tamaño mínimo de paquete



Se ha realizado una última comparativa, provocando fragmentación, superando el MTU con un paquete de 1500B, que al incrementar el paquete con las cabeceras provocará que se fragmente (*ver Figura 31)*.

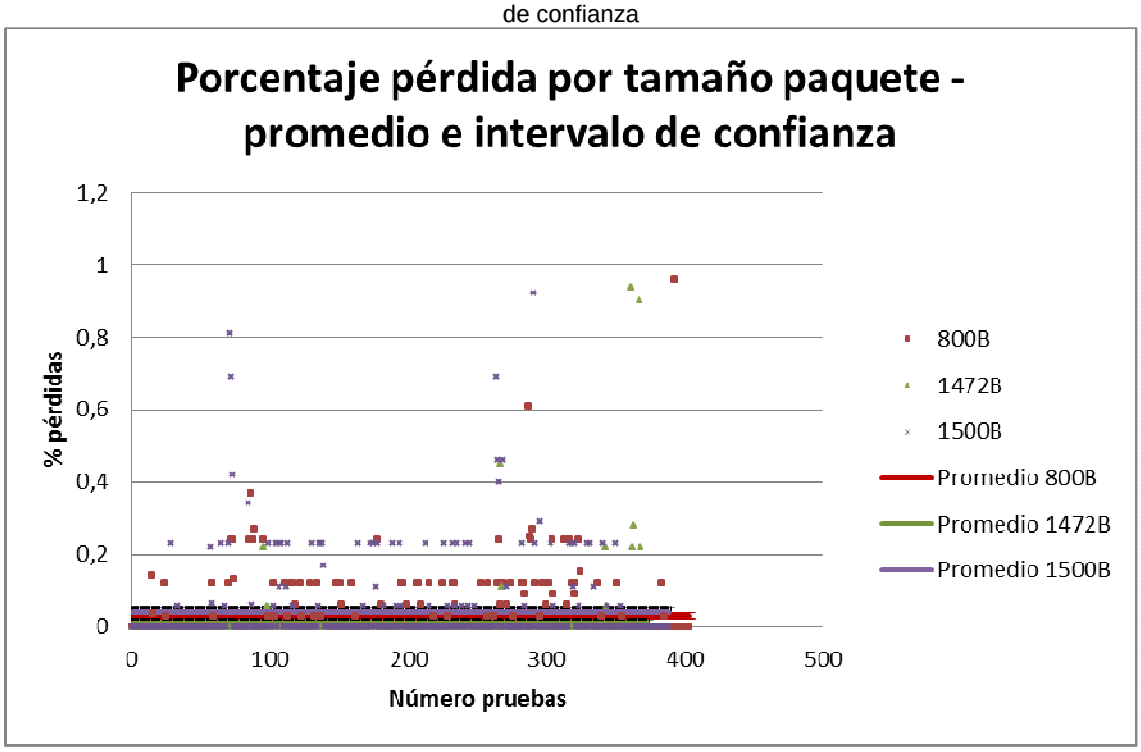
Figura 31: Porcentaje pérdida de paquetes UDP comparativa con fragmentación



Aunque el tamaño de paquete entre 1500B y 1472B es muy similar, el hecho de haber superado el MTU y que se fragmente en dos paquetes, hace que los resultados sean más similares a los obtenidos con el tamaño de paquete de 800B, ya que el número de paquetes enviados es similar.

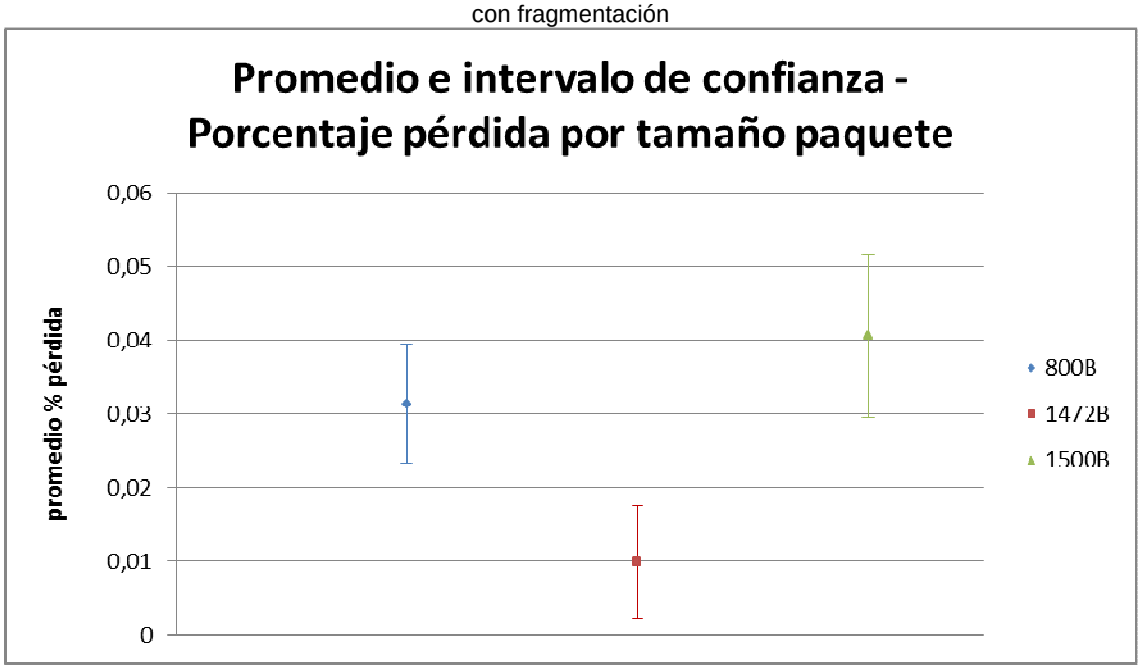
Representamos la gráfica con los promedios e intervalos de confianza *(Figura 32).*

Figura 32: Porcentaje pérdida de paquetes UDP comparativa con fragmentación – promedio e intervalos de confianza



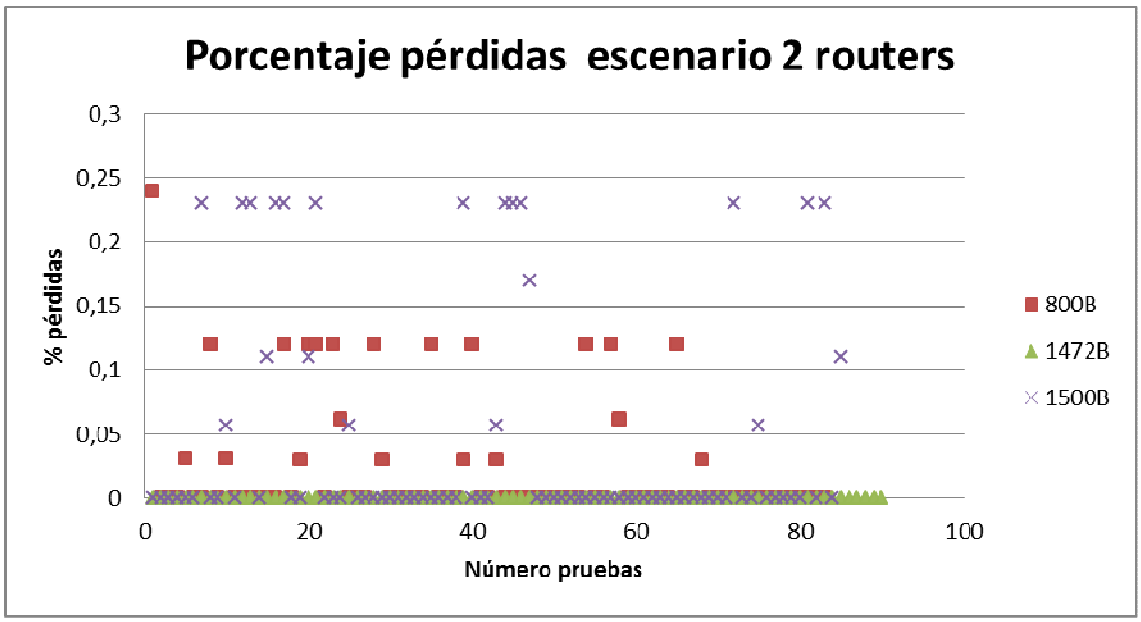
Para que pueda apreciarse mejor, representamos un único punto individual por cada promedio y su intervalo de confianza *(ver Figura 33)*.

Figura 33: Promedio e intervalo de confianza para el porcentaje pérdida de paquetes UDP comparativa con fragmentación



Si para esta comparativa aislamos el escenario más óptimo, con único salto inalámbrico y modo ad hoc (escenario con dos routers), podemos observar en la *Figura 34*, que para el tamaño máximo de paquete no tenemos pérdidas, al contrario de lo que sucede con un tamaño inferior inferior o con fragmentación (siempre para un throughput enviado en todos los casos de 1 Mbps).

Figura 34: Porcentaje pérdida de paquetes UDP escenario 2 routers

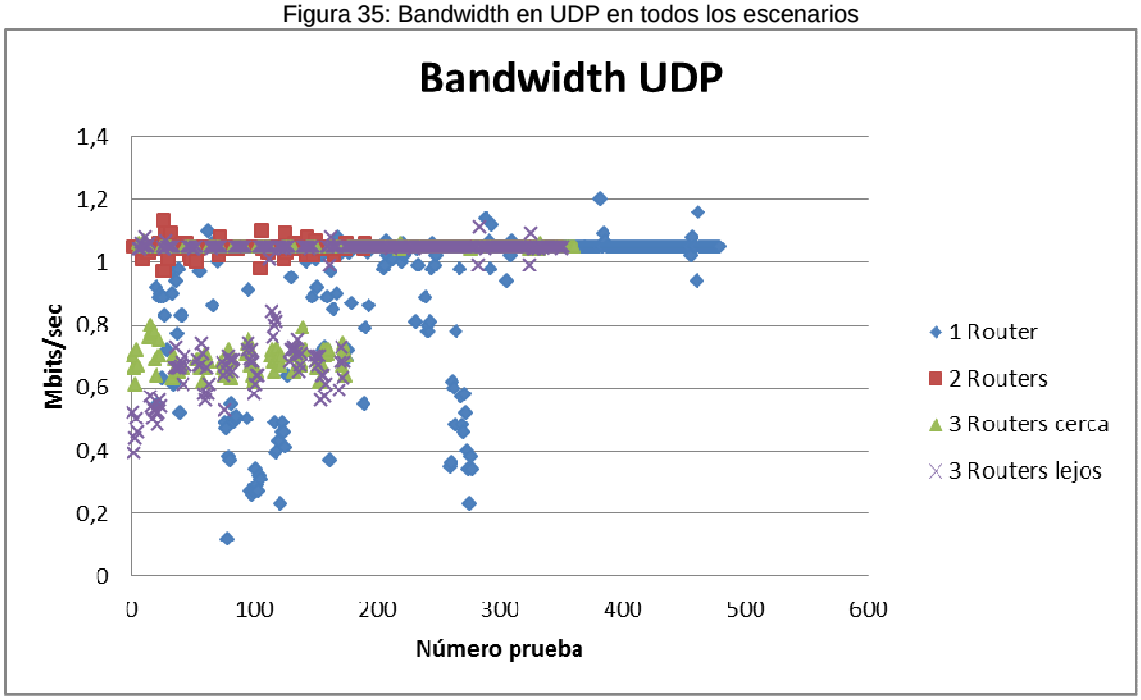


5.3.7. Throughput en UDP

Ya hemos evaluado los resultados obtenidos en función del tamaño de paquete y el porcentaje de perdidas de paquetes en UDP. Ahora se va a realizar el estudio observando el nivel de throughput obtenido en los diferentes escenarios.

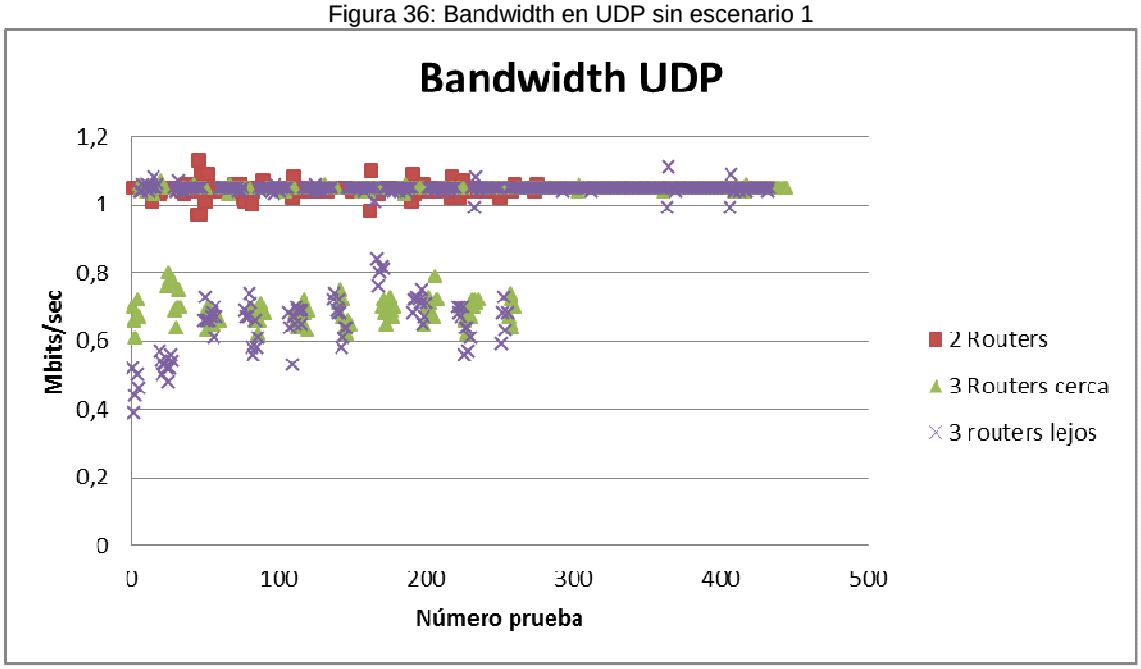
En el siguiente gráfico, representado en la *Figura 35*, se muestra el ancho de banda real obtenido en el servidor. Lo más destacable es la diferencia que se encuentra con un único salto inalámbrico pero dos configuraciones distintas, una la realizada en el escenario 1 donde teníamos un único router en modo AP y el portátil se conectaba en modo cliente, y la realizada en el escenario 2, donde se encuentran dos routers conectados en modo ad hoc y ambos PCs conectados por cable.

Figura 35: Bandwidth en UDP en todos los escenarios



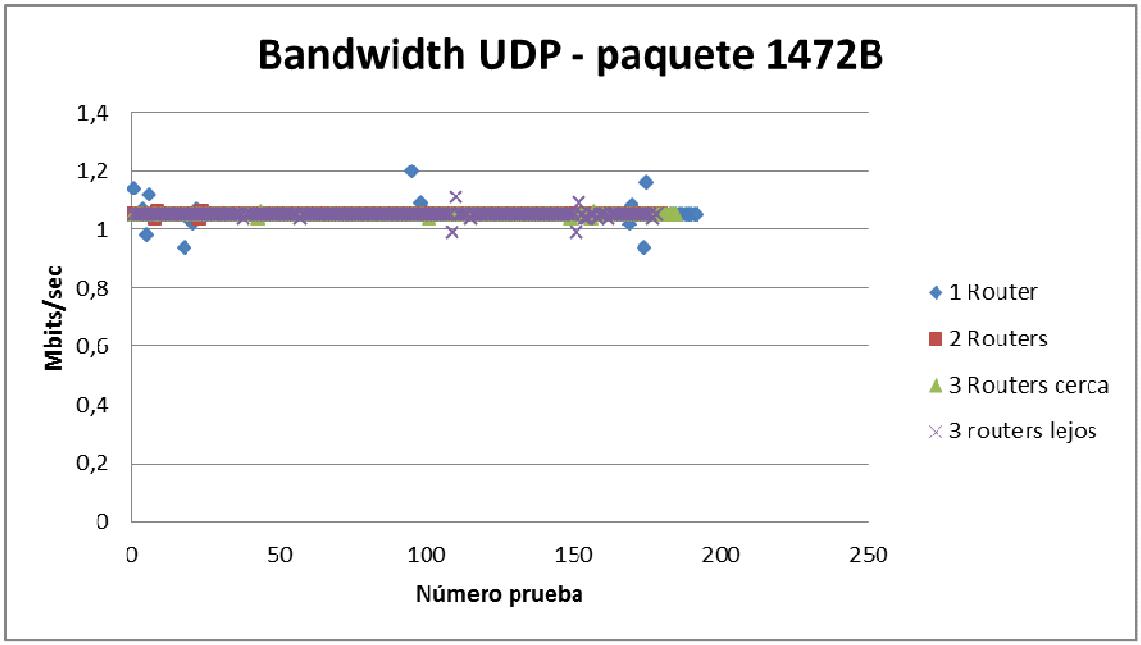
Debido a la peculiaridad del escenario 1, se representa nuevamente la gráfica sin ese escenario (*ver Figura 36)*.

Figura 36: Bandwidth en UDP sin escenario 1



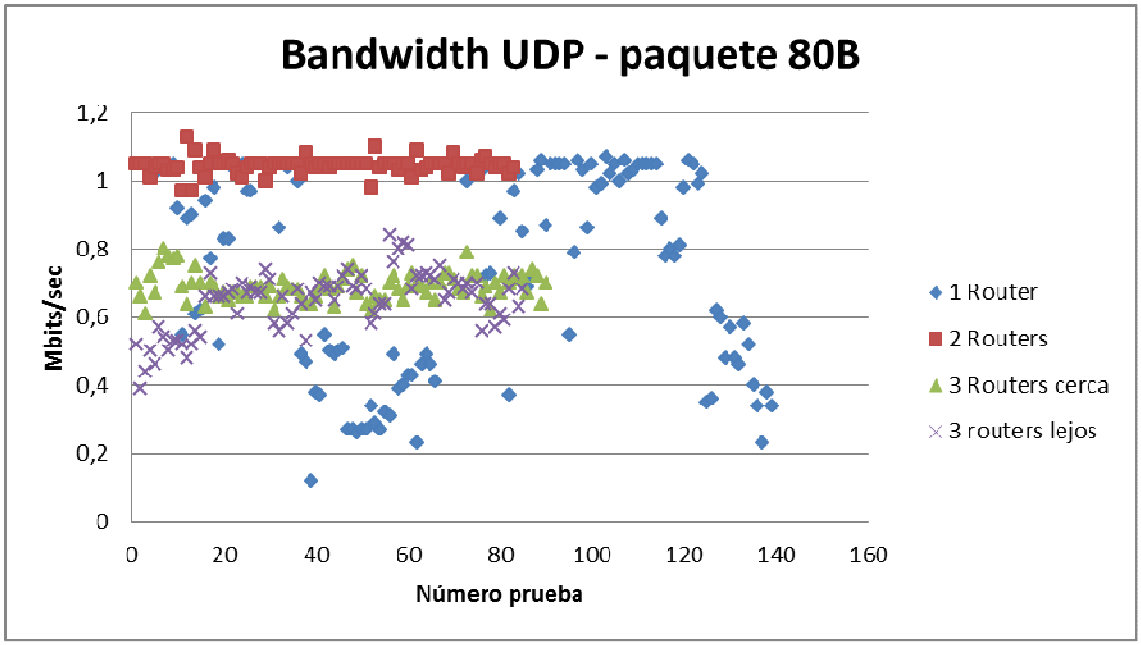
Al igual que ya vimos con las pérdidas de paquetes, obtenemos el gráfico con los datos resultado de las muestras tomadas con un tamaño de paquete de 1472B (*ver Figura 37).*

Figura 37: Bandwidth en UDP tamaño paquete 1472B



Si, en vez de con el tamaño máximo de paquete, pintamos la misma gráfica con el tamaño inferior de paquete que hemos trabajado, en la *Figura 38*, el resultado de esta gráfica es el equivalente, al de la *Figura 30*. En el escenario más óptimo, con un único salto inalámbrico en modo ad hoc, se visualiza el resultado más favorable, al no tener practicamente pérdidas de paquetes, el bandwidth que se obtiene es aproximado al enviado por el cliente, 1Mbits/sec, en el resto de escenarios, el bandwidth se degrada en función de los paquetes perdidos.

Figura 38: Bandwidth en UDP tamaño paquete 80B



Representamos la misma gráfica con los promedios e intervalos de confianza. Eliminamos el escenario de un router en modo infraestructura por se un caso particular (*ver Figura 39 y Figura 40*).

Figura 39: Bandwidth en UDP tamaño paquete 80B - promedio e intervalo de confianza

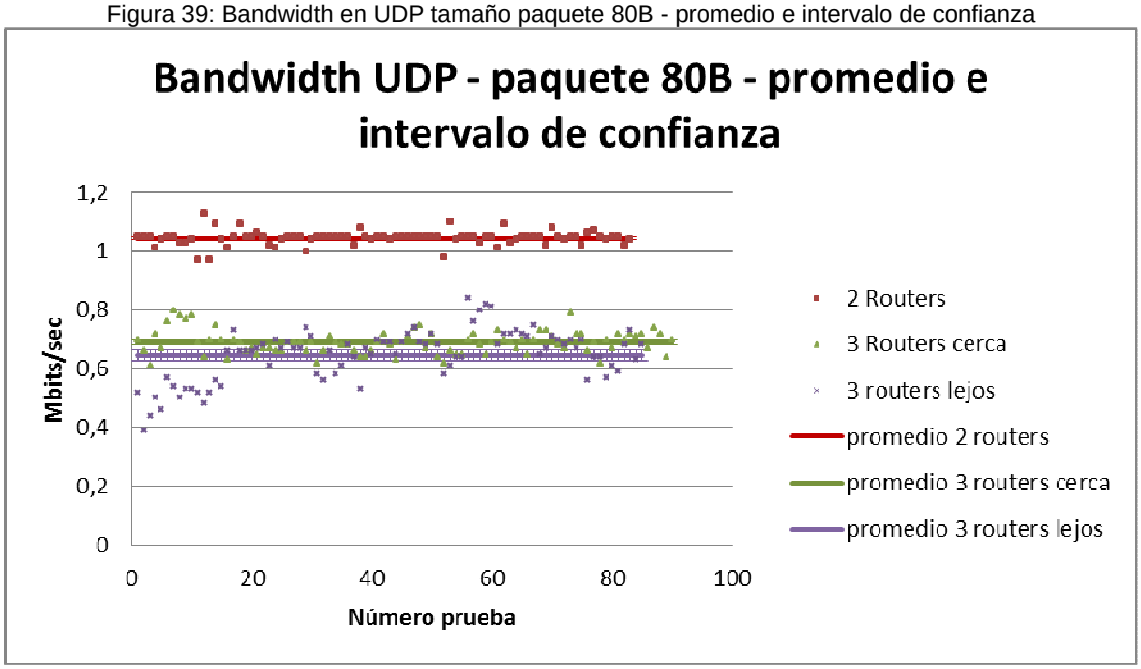
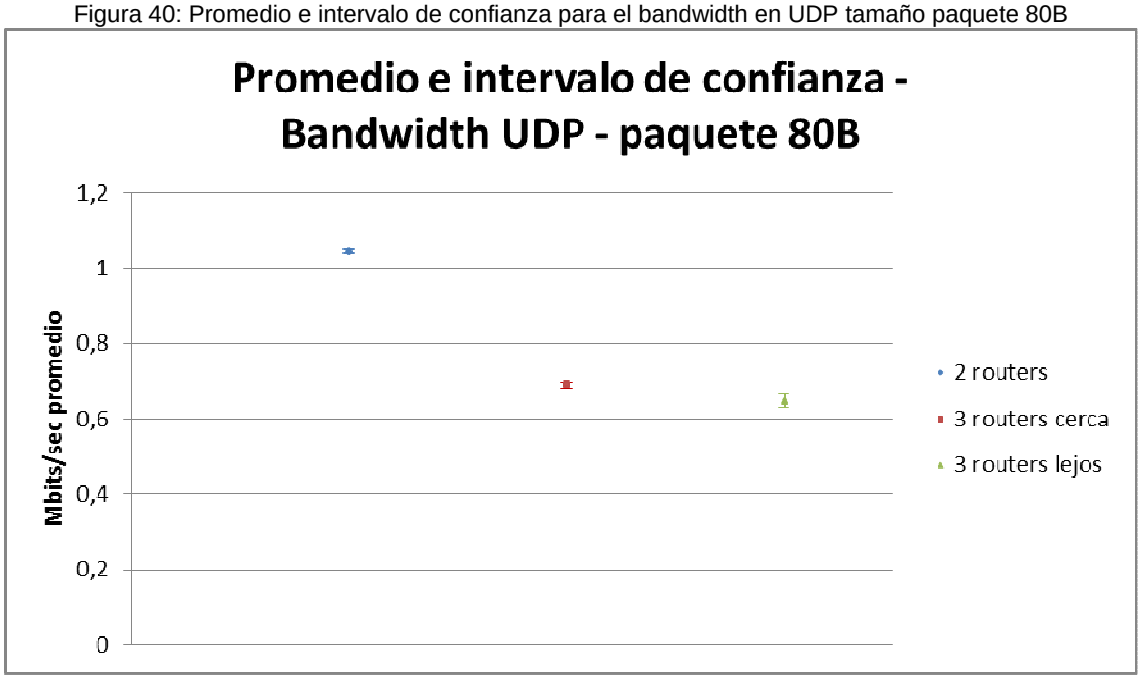


Figura 40: Promedio e intervalo de confianza para el bandwidth en UDP tamaño paquete 80B



Si mostramos el bandwidth en función del tamaño de paquete, en vez por escenario, concuerda con los resultados mostrados en la *Figura 27*, para las pérdidas de paquetes en función del tamaño de paquete enviado (*ver Figura 41)*. Se representa la misma gráfica añadiendo las muestras obtenidas con fragmentación y eliminando las muestra obtenidas con el tamaño de paquete de 80B, para poder comparar de manera más representativa entre ellas (*ver Figura 42*).

Figura 41: Bandwidth en UDP por tamaño paquete

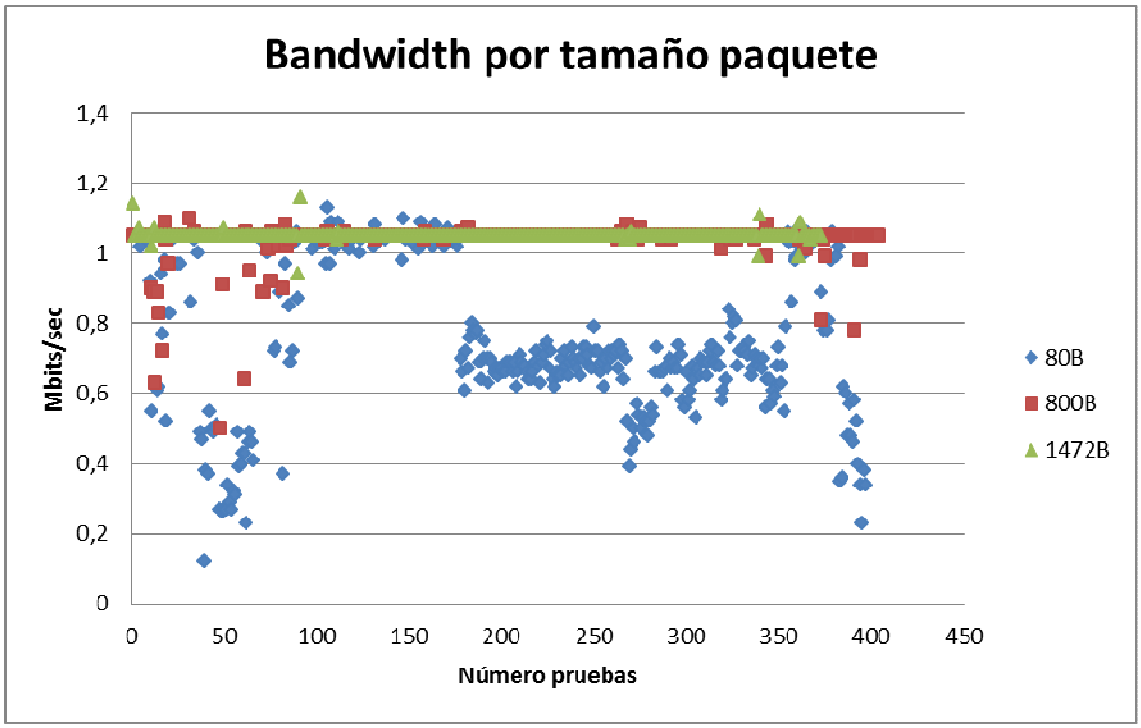
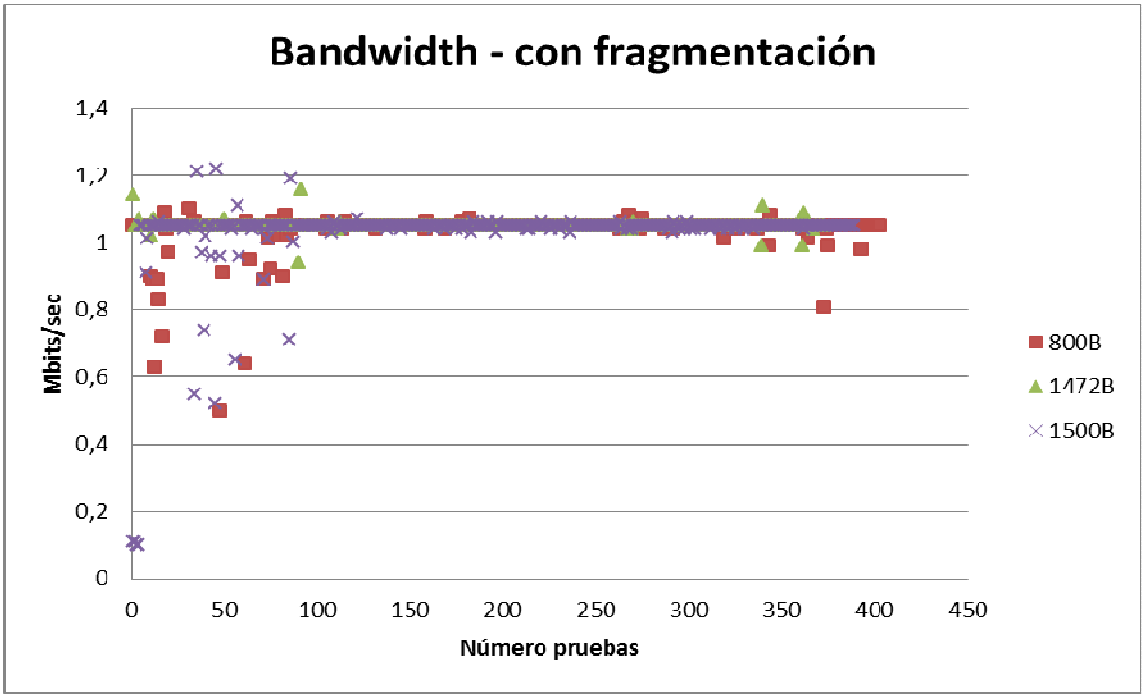


Figura 42: Bandwidth en UDP por tamaño paquete con fragmentación



5.3.8. Throughput y pérdidas en UDP con 15Mbits/sec

Como el throughput enviado por el cliente por defecto en iperf es 1Mbits/sec, se ha realizado un nuevo experimento en todos los escenarios aumentando el caudal de envío a 15Mbits/sec.

Figura 43: Porcentaje pérdida de paquetes con envío de 15Mbits/sec

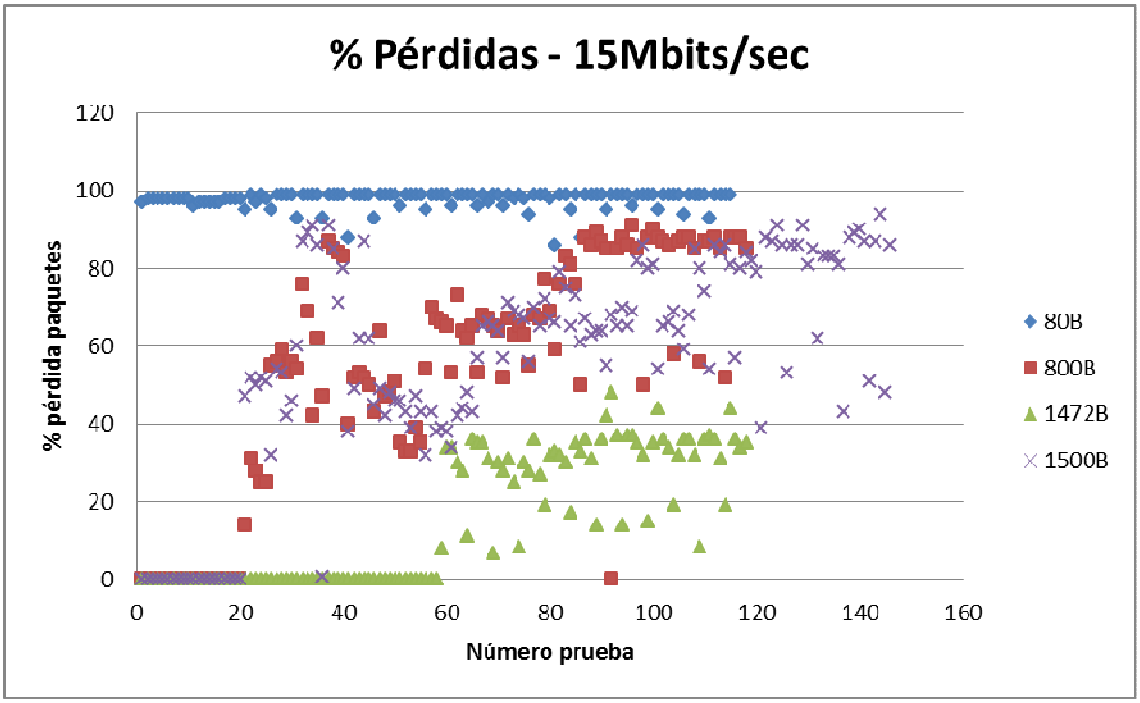
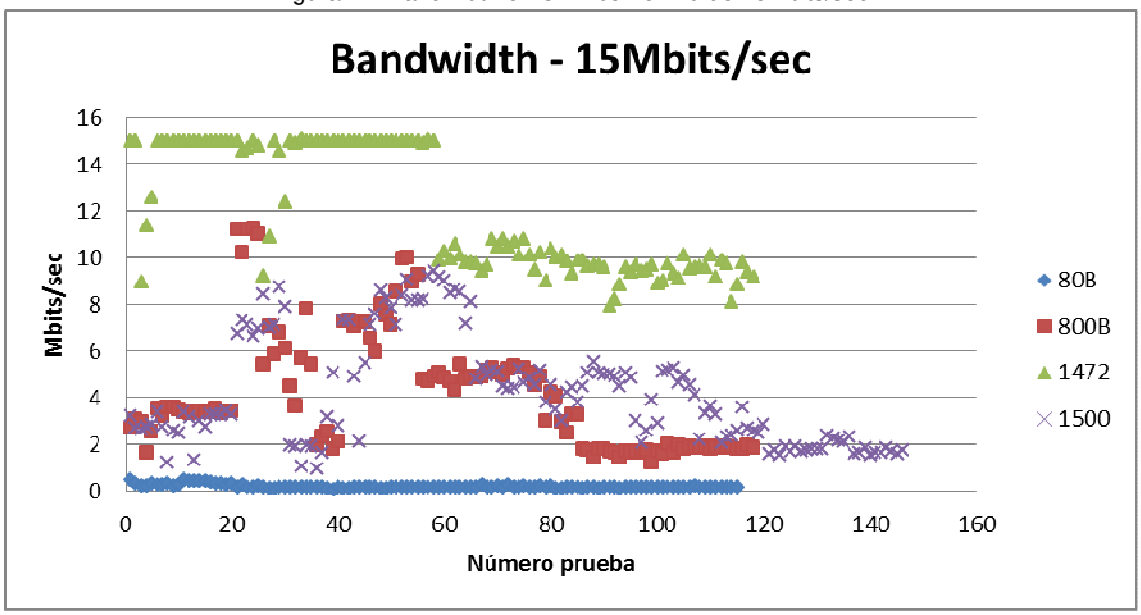


Figura 44: Bandwidth en UDP con envío de 15Mbits/sec



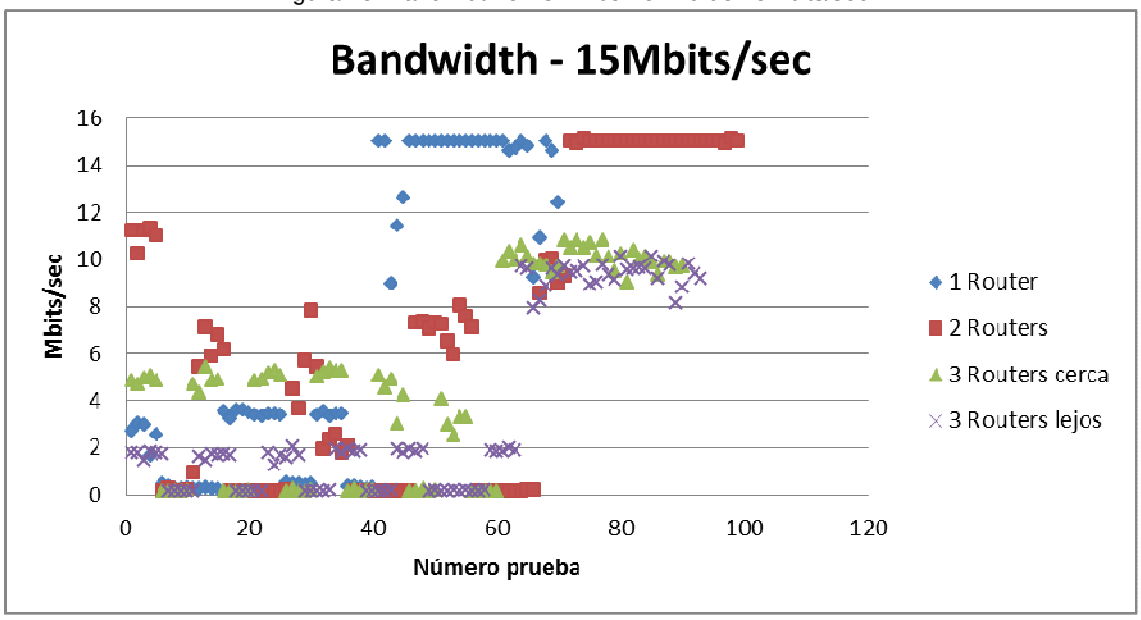
En las *Figura 43 y Figura 44*, se han tenido en cuenta todos los tamaños de paquete utilizados, un tamaño de paquete pequeño, uno intermedio, un máximo y uno que provoque fragmentación. En estos gráficos están representado todos los escenarios, en *Figura 45, Figura 46 y Figura 49* se separara por casuística de nodos inalámbricos. En estas primeras gráficas, representadas en las *Figuras 35* y *36*, puede observarse que con un tamaño pequeño, este aumento de cuadal, perjudica notablemente llegado casi a perder el 100% de los paquetes. Obteniendo un throughput inferior respecto al que se obtenía cuando el inicial era 1 Mbits/sec.

Las muestras para el tamaño de paquete intermedio y el obtenido con fragmentación, como ya se ha visto en los apartados anteriores, es similar.

Como era de esperar, los mejores resultados son los obtenidos con el tamaño de paquete mayor.

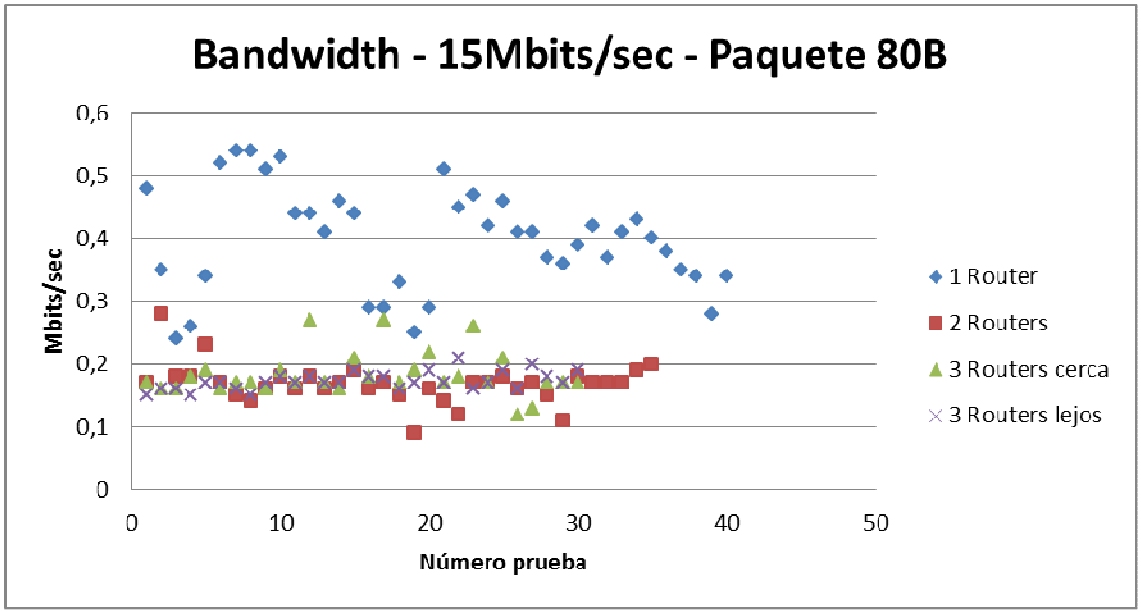
En la siguiente gráfica, se representan los mismos datos, pero separado por el número de nodos inalámbricos y su casuística (*ver Figura 45*).

Figura 45: Bandwidth en UDP con envío de 15Mbits/sec



Al estar resprentadas las muestras con todos lo tamaños de paquete, es un poco confusa la visualización de la gráfica, aunque, los puntos más altos, es decir, los casos de mayor bandwidth, son los obtenidos con el tamaño de paquete mayor, y los puntos inferiores son los obtenidos con el tamaño de paquete inferior. Para poder visualizarlo mejor, reprentamos el resultado separado por el tamaño de paquete (*ver Figura 46 y Figura 49)*.

Figura 46: Bandwidth en UDP con envío de 15Mbits/sec con paquetes de 80B



Representamos la misma gráfica con los promedios e intervalos de confianza en la *Figura 47* y de forma individual en la *Figura 48.*

.

Figura 47: Bandwidth en UDP con envío de 15Mbits/sec con paquetes de 80B – promedios e intervalos de confianza

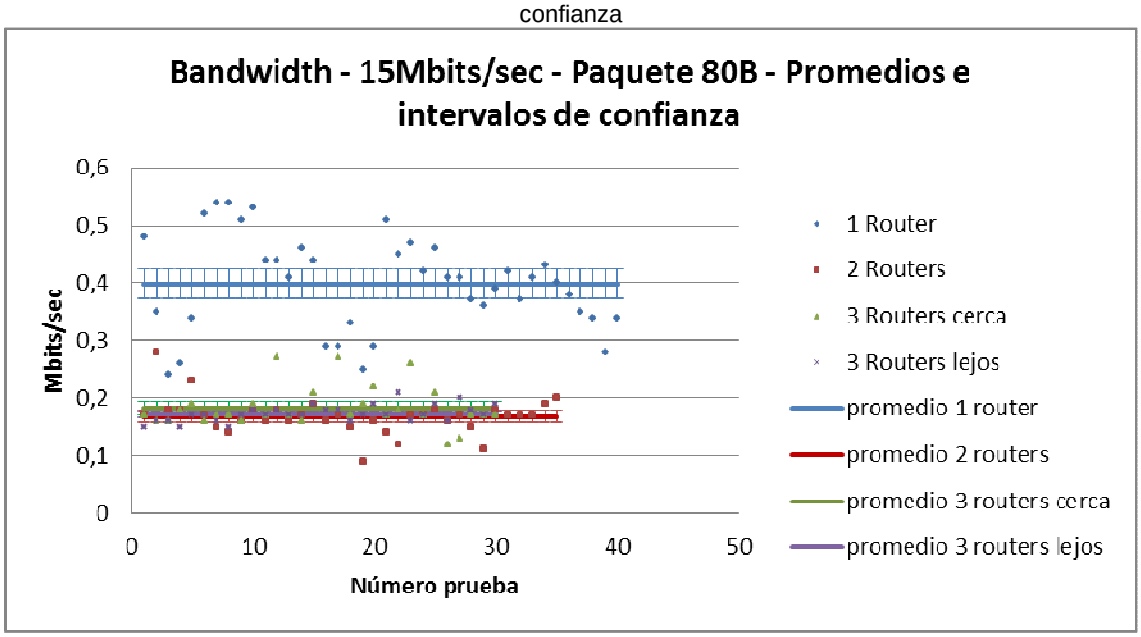
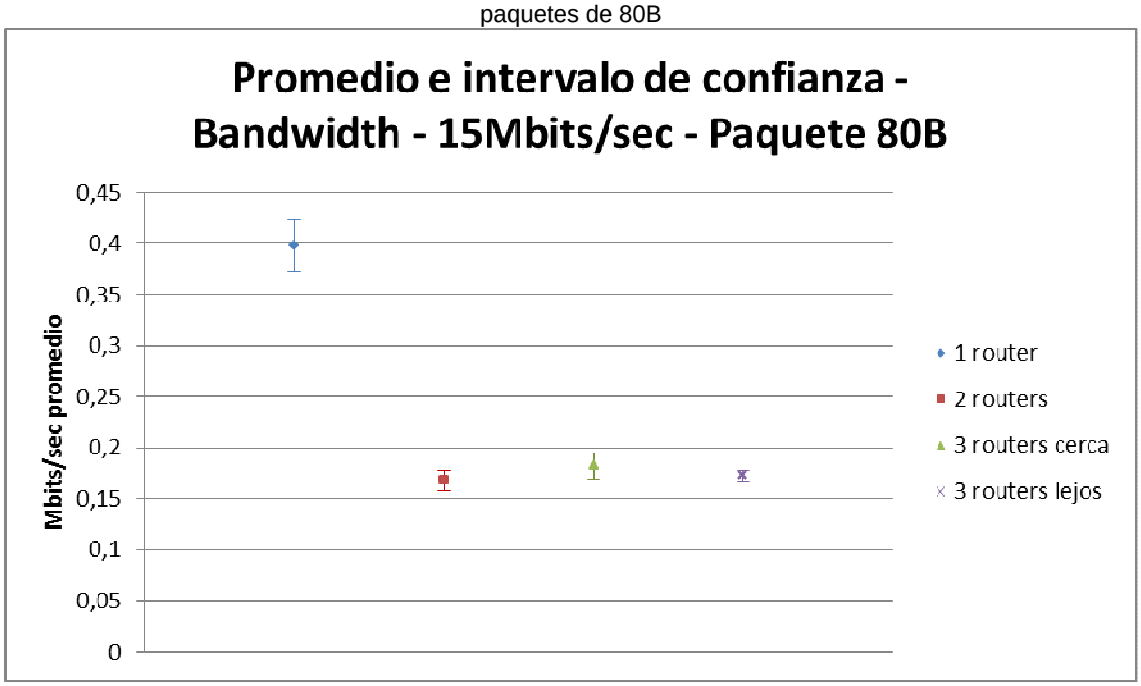


Figura 48: Promedio e intervalo de confianza para el bandwidth en UDP con envío de 15Mbits/sec con paquetes de 80B



Para el tamaño de paquete de 1472B obtenemos también su gráfica (*Figura 49*), incluyendo los promedios e intervalos de confianza (*Figura 50*) y representados de forma individual (*Figura 51*).

Figura 49: Bandwidth en UDP con envío de 15Mbits/sec con paquetes de 1472B

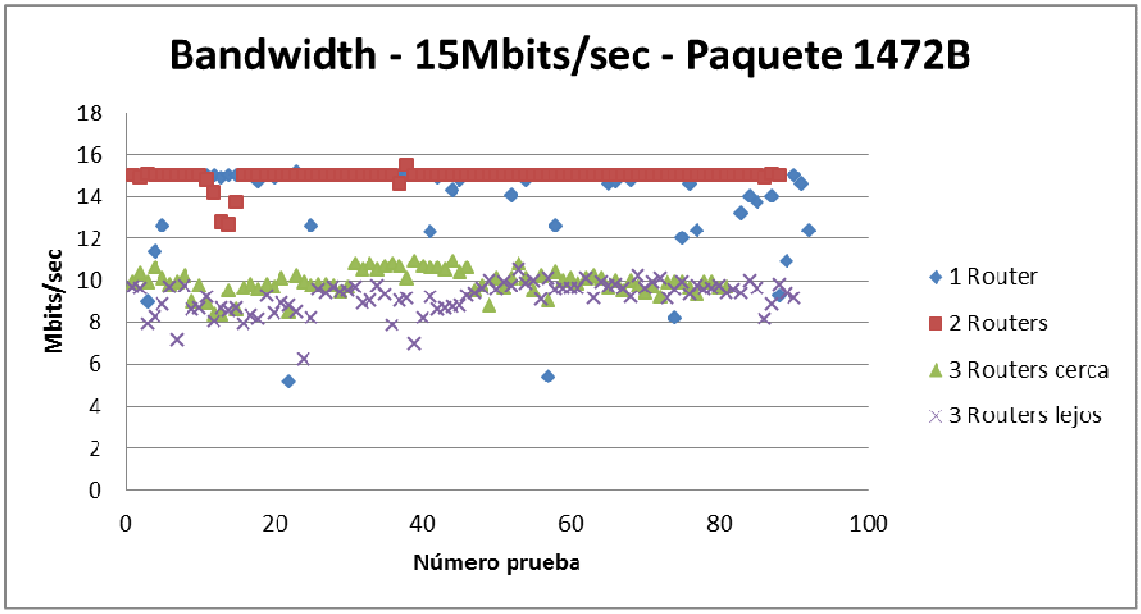


Figura 50: Bandwidth en UDP con envío de 15Mbits/sec con paquetes de 1472B – promedios e intervalos de confianza

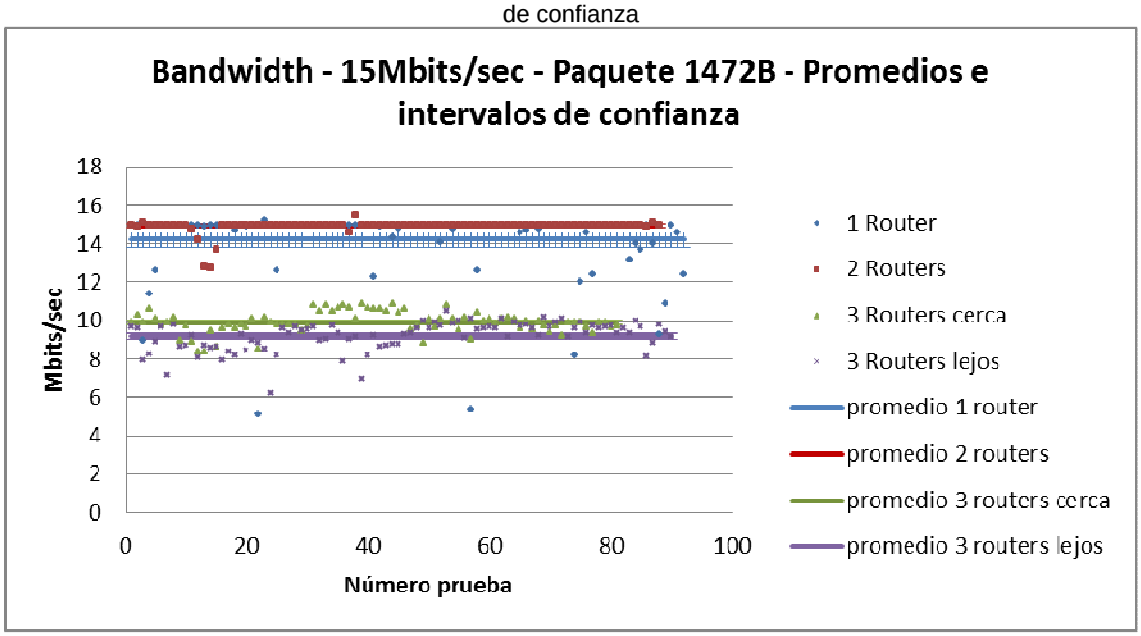
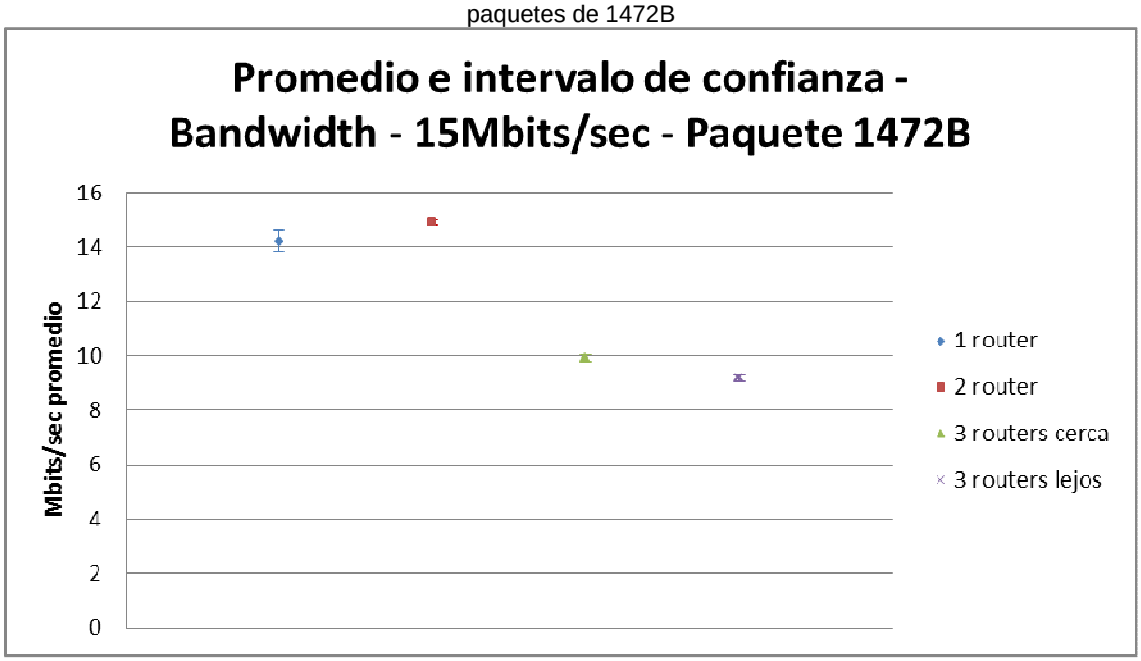


Figura 51: Promedio e intervalo de confianza para el bandwidth en UDP con envío de 15Mbits/sec con paquetes de 1472B



Al igual que se ha representado por escenarios en througthput, se visualizan la pérdida de paquetes de la misma manera (*ver Figura 52, Figura 53 y Figura 54)*.

Figura 52: Porcentaje pérdidas en UDP con envío de 15Mbits/sec

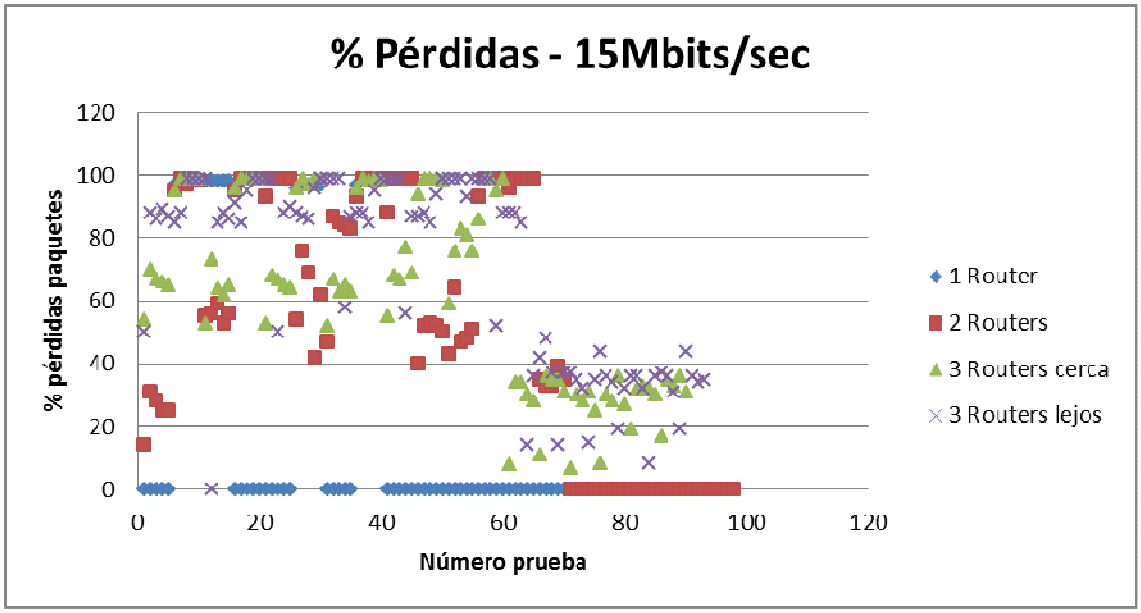


Figura 53: Porcentaje pérdidas en UDP con envío de 15Mbits/sec con paquetes de 80B

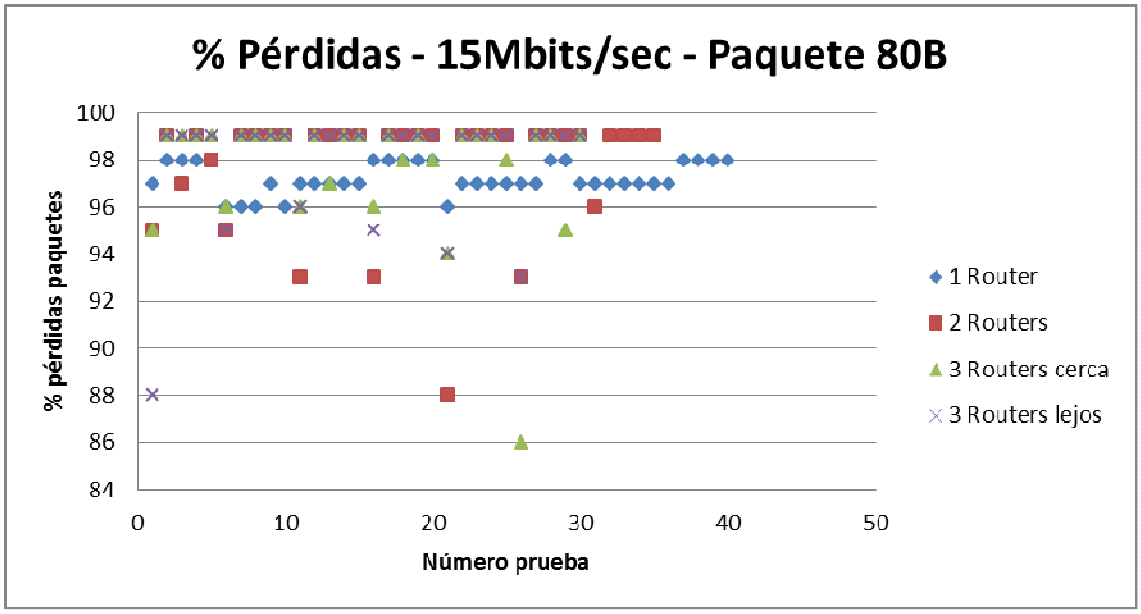
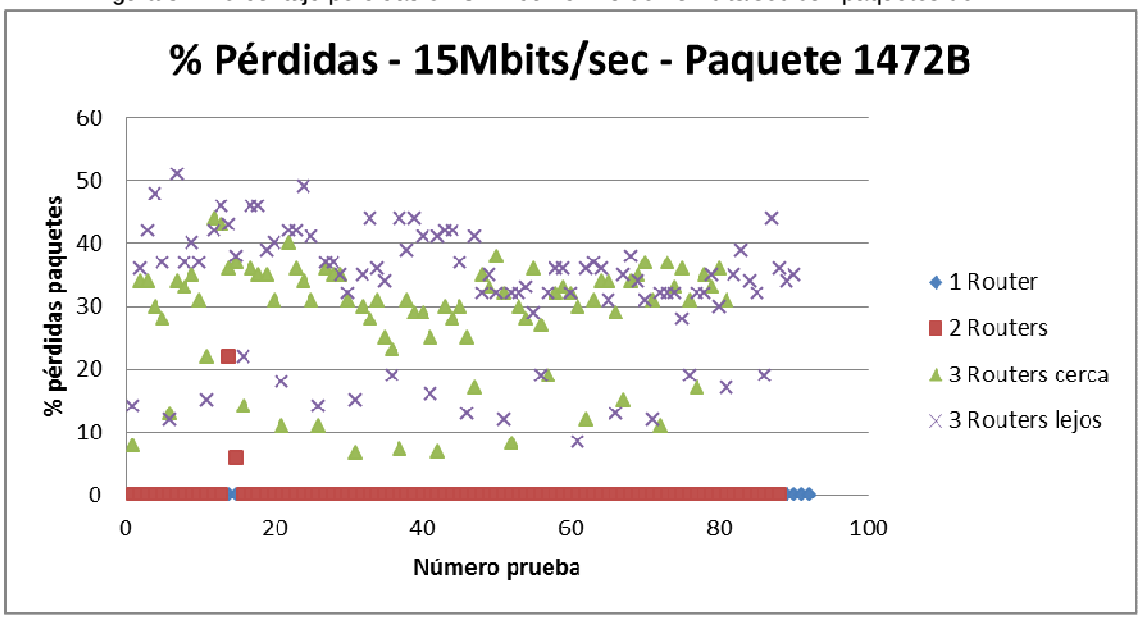


Figura 54: Porcentaje pérdidas en UDP con envío de 15Mbits/sec con paquetes de 1472B



Seleccionando las gráficas que respresentan las muestras obtenidas con el paquete de tamaño mayor (*ver Figura 53 y Figura 54*), puede verse claramente, que el escenario más favorable, al igual que con un envío por parte del cliente de 1 Mbits/sec, es con único salto inalámbrico en modo ad hoc y dos routers. Aunque puede verse que este caso, el salto inalámbrico con un único router en modo infraestructura, mejora respecto de las anteriores pruebas. Al añadir más saltos inalámbricos, las pérdidas aumentan, provocando un menor througthput final, siendo más notable, cuando están más alejados los nodos.

5.3.9. Throughput y pérdidas en UDP con tráfico bidireccional

Como ya vimos en la parte TCP, se han realizado pruebas con tráfico bidireccional, en este caso como el ancho de banda por defecto con el comando iperf es 1Mbit/sec, algo que podemos comprobar en las gráficas anteriores donde vemos que las mejores muestras se mantienen en ese número, se ha reducido en cada caso a 500Kbit/sec, para que el ancho de banda total sumando el tráfico de ambas direcciones sea igual al anterior.

A diferencia con TCP, en UDP, el tráfico sí es realmente unidireccional en las primeras pruebas ya que no manda ningún ACK de confirmación.

Dado que el escenario 1 daba unos resultados diferentes a los obtenidos con la configuración ad hoc, para esta comparativa lo hemos eliminado de la gráfica (*ver Figura 55)*.

Figura 55: Bandwidth en UDP con tráfico bidireccional, representado por tamaño de paquete

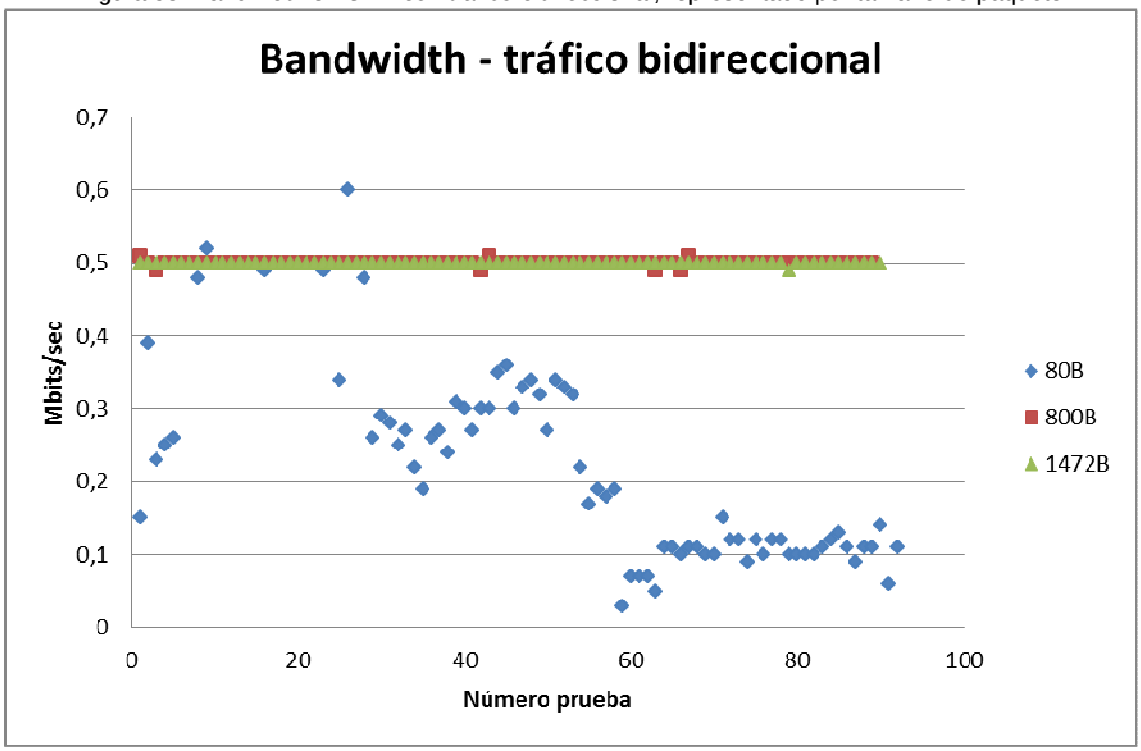


Figura 56: Porcentaje pérdida de paquetes en UDP con tráfico bidireccional, representado por tamaño paquete.

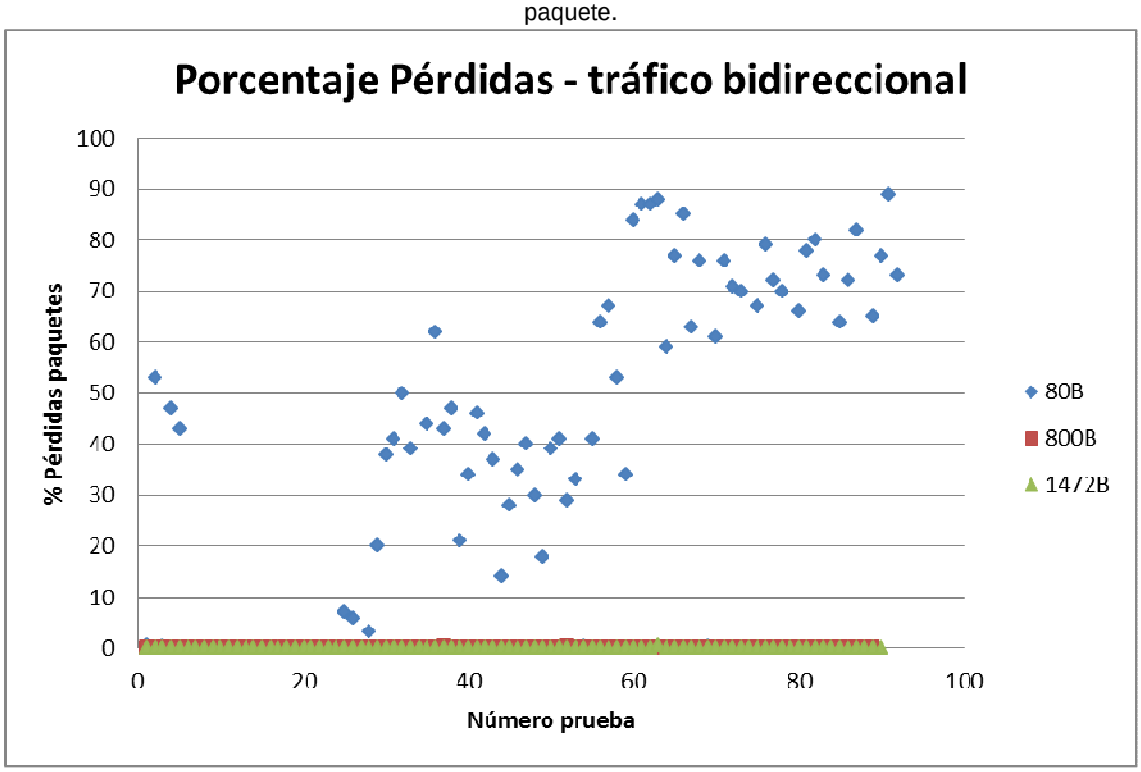


Figura 57: Bandwidth en UDP con tráfico bidireccional, representado por escenario

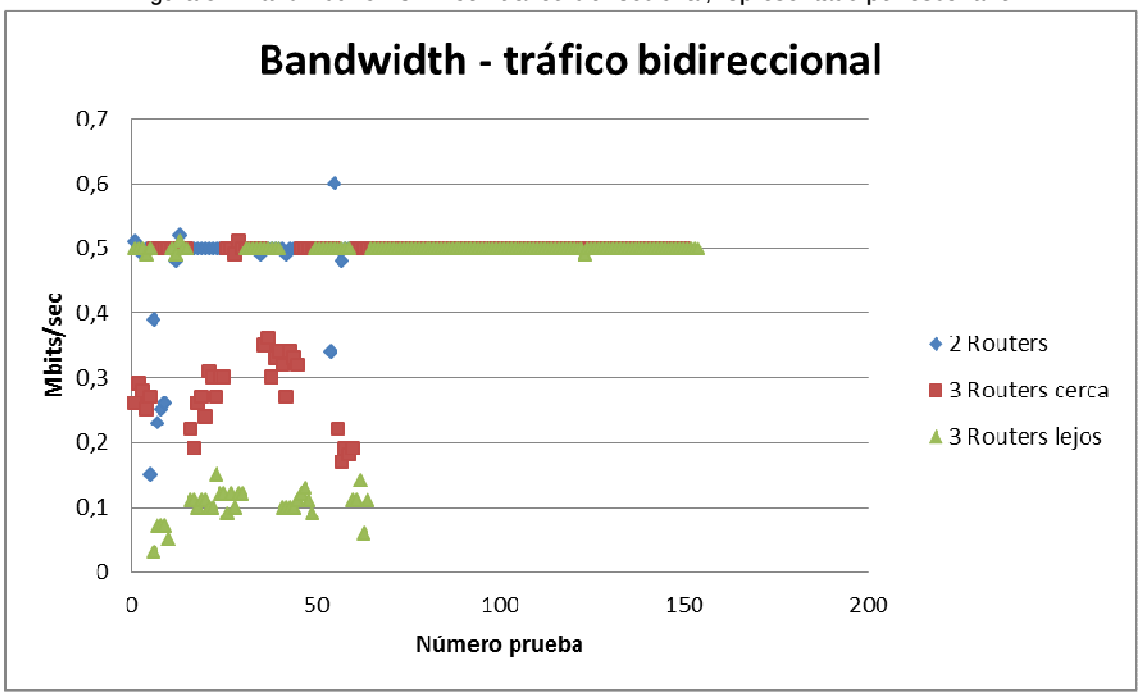
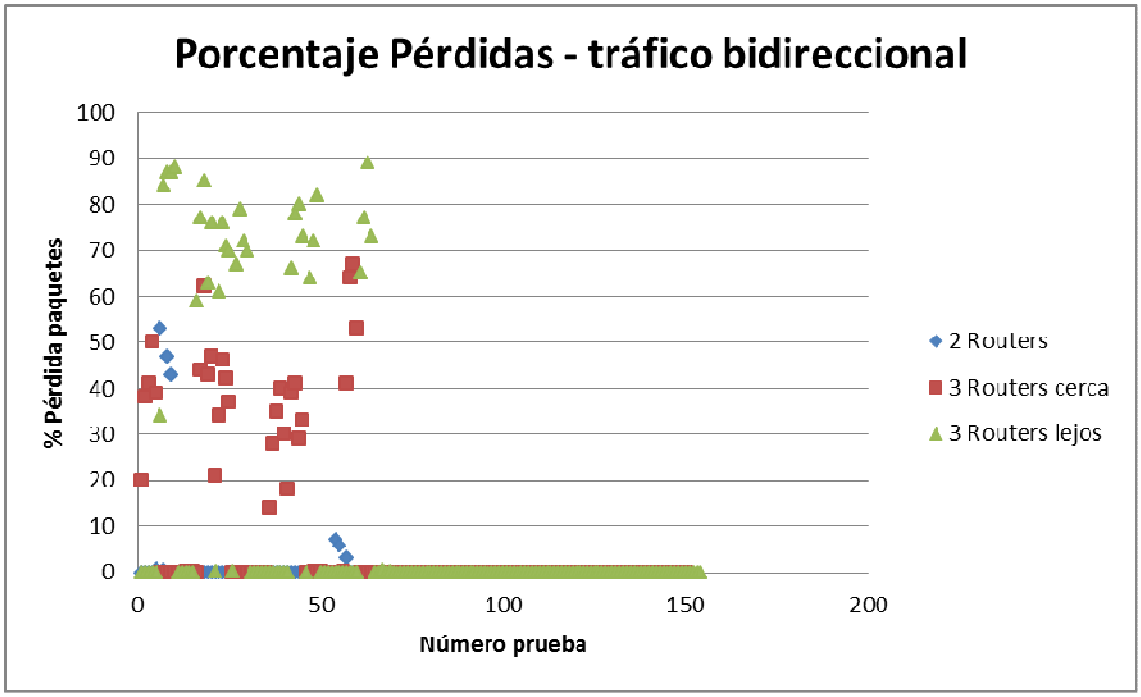


Figura 58: Porcentaje de pérdida de paquetes en UDP con tráfico bidireccional, representado por escenario



En las *Figura 55 y Figura 56*, puede apreciarse que para los tamaños de paquetes intermedio y máximo, se mantiene estable el througthput sin apenas pérdidas de paquetes, al contrario de lo que sucede con un tamaño de paquete inferior. Para poder obtener más detalle sobre el caso del tamaño de paquete de 80B, lo separamos del resto de muestras y lo evaluamos por escenario (*ver Figura 59 y Figura 60*).

Figura 59: Bandwidth en UDP con tráfico bidireccional para paquetes de 80B

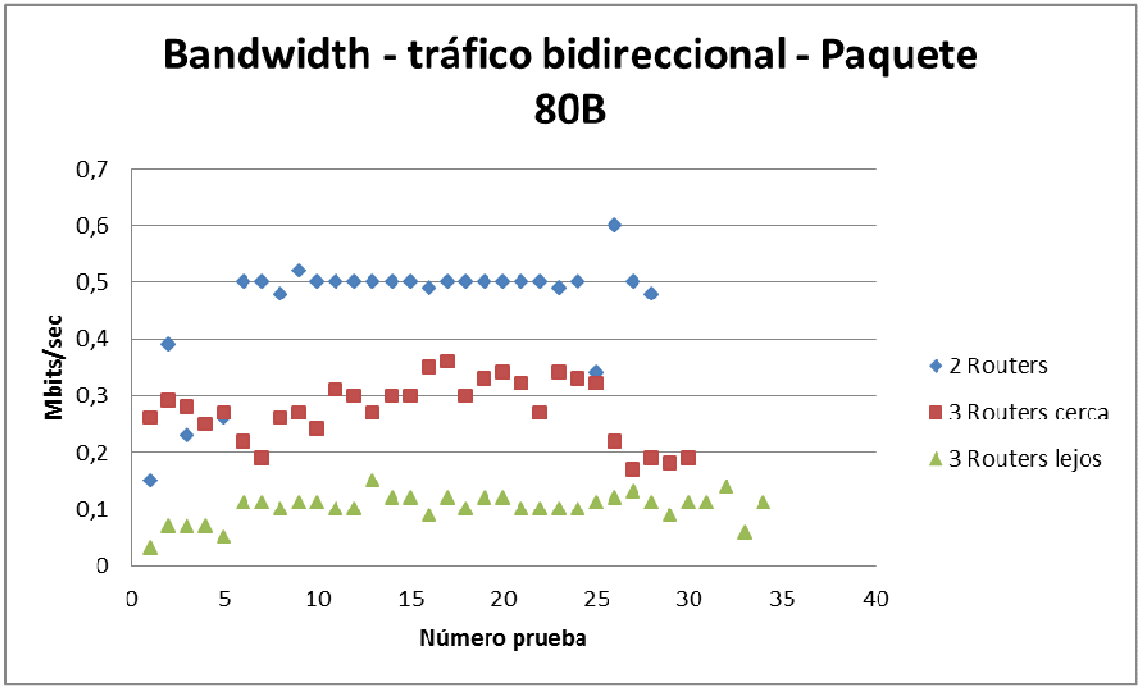
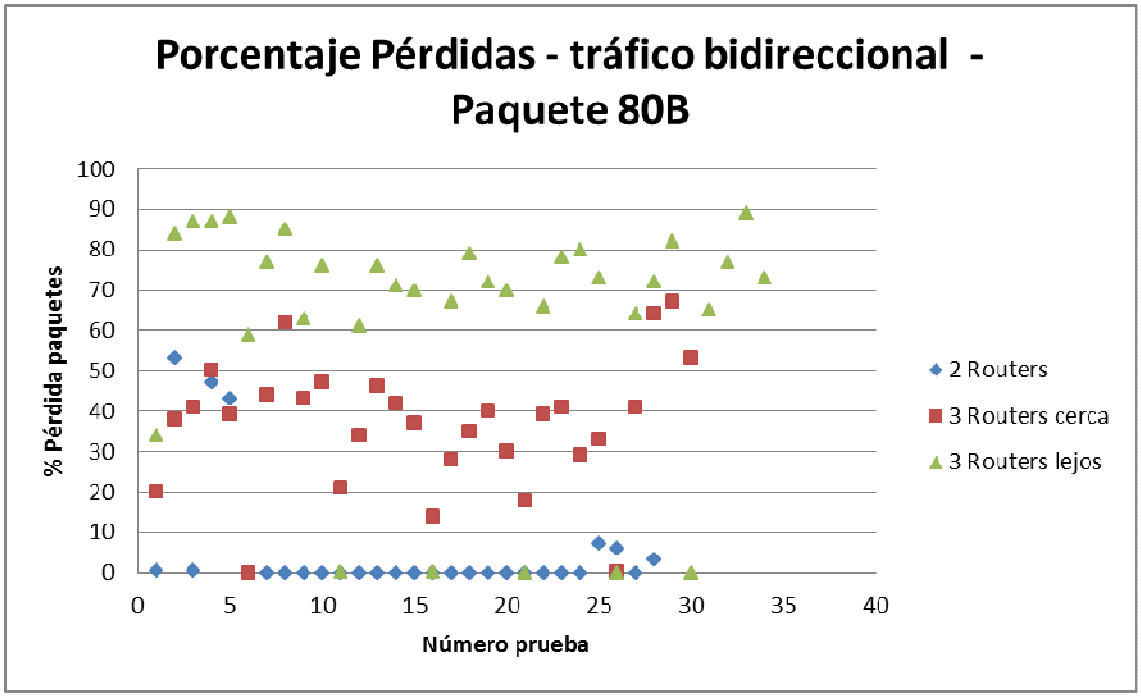


Figura 60: Porcentaje pérdida de paquetes en UDP con tráfico bidireccional para paquetes de 80B



Representamos la *Figura 59* con los promedios e intervalos de confianza en la *Figura 61* y de forma individual en la *Figura 62*.

Figura 61: Bandwidth en UDP con tráfico bidireccional para paquetes de 80B - promedios e intervalos de confianza

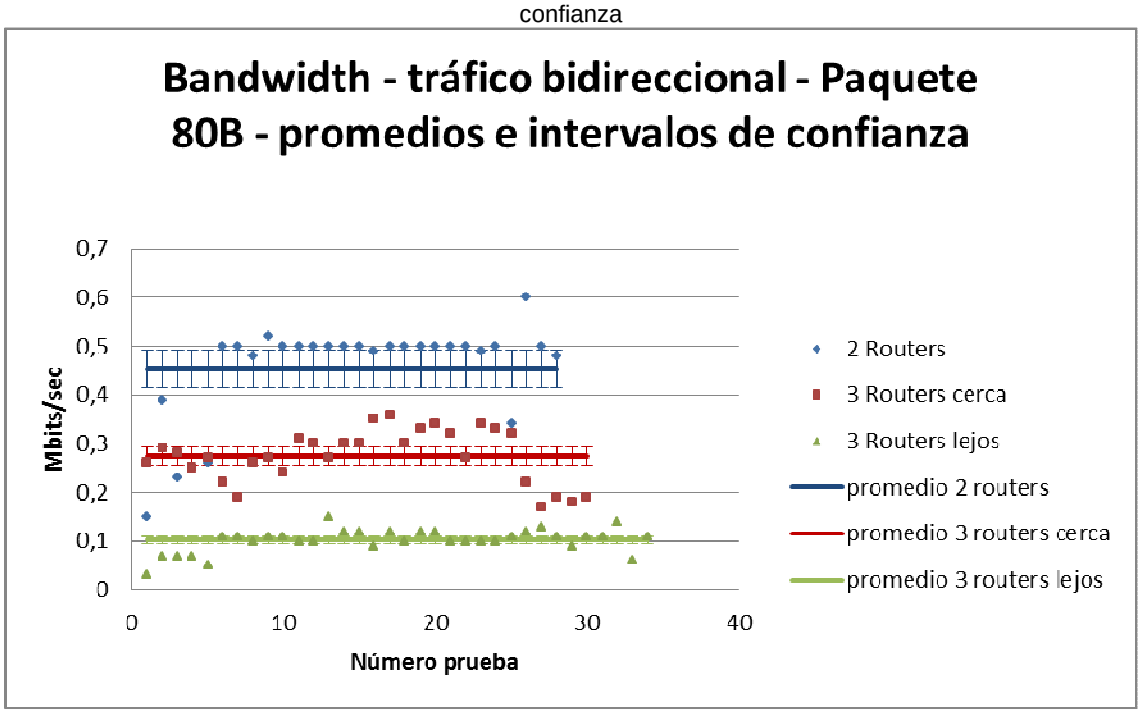
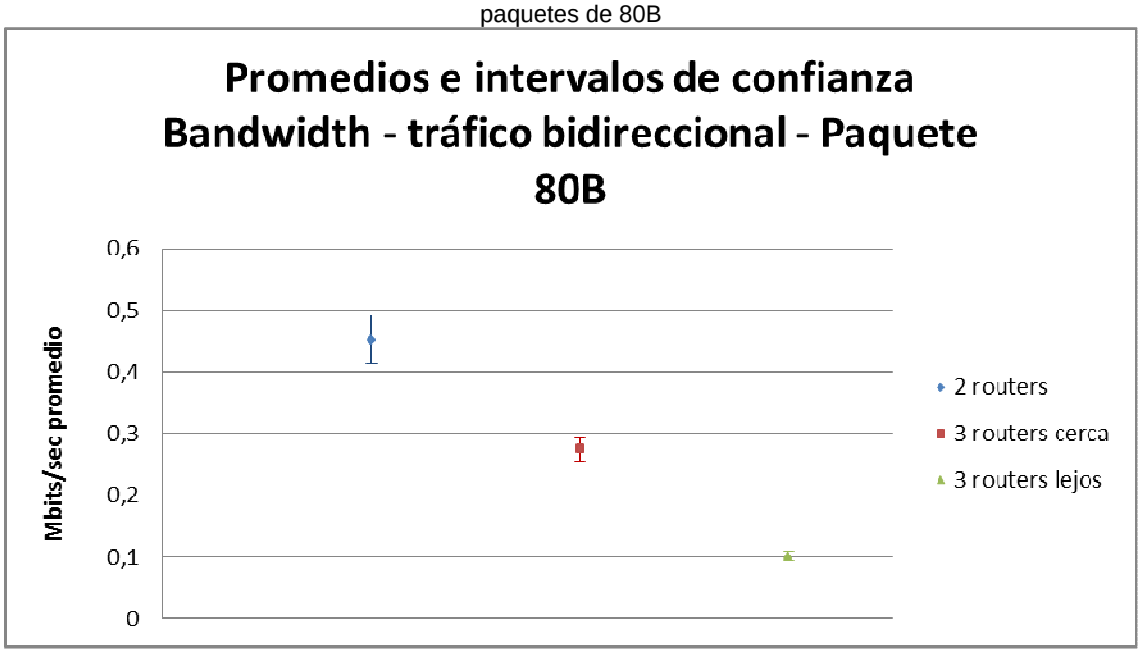


Figura 62: Promedio e intervalo de confianza para le bandwidth en UDP con tráfico bidireccional para paquetes de 80B



Se puede comparar las figuras de throughput TCP con tráfico de datos unidireccional (*Figura 17*) y con tráfico bidireccional (*Figura 26*) con el caso UDP para paquetes de 80 B (*Figura 39 y Figura 62*). Lo que se aprecia es que, en general, aumentar el número de routers intentando enviar tráfico penaliza las prestaciones aunque el tráfico total en la red sea el mismo.

Una vez realizadas todas las pruebas y representadas en gráficos podemos realizar su evaluación y dictaminar unas conclusiones.

5.4 Conclusiones pruebas

Después de evaluar todos los resultados de las pruebas las principales conclusiones son:

- El incremento de saltos inalámbricos empeora notablemente el throughtput del envío de paquetes. El escenario más óptimo es un único salto inalámbrico en modo ad hoc, reduciendose a la mitad el througthput simplemente añadiendo un salto más.

- En UDP, realizar los envíos con un tamaño de paquete pequeño incrementa el porcentaje de pérdidas de esos paquetes, ya que el número de paquetes a enviar para mandar la misma cantidad de datos es mayor. Al incrementar el número de paquetes pérdidos se decrementa el througthput obtenido. Alcanzándose los mejores resultados con el tamaño de paquete máximo sin fragmentación que permite el MTU.

- Al generar tráfico similar en ambos sentidos, el througthput se reduce ya que ambos envíos deben competir por el medio inalámbrico. Esto sucede tanto en TCP como en UDP, aunque en TCP, como ya comentamos siempre existe tráfico bidireccional, debido al envío de ACKs. Por lo que se ha podido observar, el escenario más impactado en ambos casos es el de 3 routers con mayor lejanía entre ellos.

- Al incrementar el througthput de entrada en UDP, a 15Mbits/sec, se incrementa el porcentaje de paquetes pérdidos en todos los escenarios. De hecho, con 15 Mbit/s de entrada en UDP (unidireccional) y tamaño de paquete el máximo que no provoca fragmentación, el throughput efectivo es superior al obtenido en TCP (como era de esperar, por el mecanismo de control de congestión de TCP pero también por la ausencia en UDP de tráfico de asentimientos que penalizan por la competencia por el medio inalámbrico). Con un salto inalámbrico la diferencia no es muy grande (12,05 Mbit/s en TCP y casi 15 Mbit/s en UDP) pero sí es mucho mayor con dos saltos inalámbricos (5 Mbit/s en TCP y casi 10 Mbit/s en UDP). Todo esto confirma que según se aumenta la competencia por el medio (varios routers diferentes teniendo tráfico a enviar simultáneamente) el uso del medio es cada vez más ineficiente.

- En los escenarios evaluados no se aprecia diferencia entre los resultados obtenidos en diferentes canales de frecuencia, ni usando diferente potencia de transmisión.

6. Conclusiones

Una vez finalizado este proyecto podemos concluir con la importancia que tiene realizar estudios sobre las redes inalámbricas multi-salto ya que, como ya comentamos al inicio del proyecto, existen múltiples casuísticas y, como se ha visto en las pruebas, los resultados varían en función de ellas.

Para poder instalar una red inalámbrica multi-salto óptima hay que tener en cuenta todos los factores: la distancia, el número de nodos, los parámetros de esos nodos, etc. De esta manera intentar conseguir un equilibrio entre la versatilidad de tener múltiples nodos, pero a la vez no perder rendimiento.

Hemos podido observar en las pruebas cómo afecta al rendimiento la inclusión de más nodos o la distancia entre ellos. Hemos confirmado cómo aumentar el número de routers en la red que compiten por el medio (tienen tráfico para enviar simultáneamente) hace que la eficiencia en el uso del medio baje y el throughput global de la red se reduzca. Esto ocurre, por ejemplo, cuando tenemos varios saltos inalámbricos y/o con tráfico bidireccional. También hemos confirmado el efecto del tamaño de paquete en las prestaciones de la red inalámbrica, siendo más costoso enviar el mismo tráfico con paquetes más pequeños.

También se ha llegado a la conclusión de la importancia que tiene automatizar las tareas más tediosas y repetitivas. Parte fundamental en un experimento basado en la toma de datos. Es clave señalar para futuros investigadores la importancia de estructurar las pruebas con el objeto de que dicha automatización sea una tarea óptima, sencilla y fácilmente escalable.

Asimismo es importante dejar reflejado como parte del aprendizaje adquirido y como reseña a futuros estudiantes la significativa importancia que cobra un buen diseño de pruebas y toma de datos. En nuestro experimento hubo que repetir la toma de datos al errar la consideración del tamaño del paquete y no tener en cuenta cabeceras, lo cual provocaba fragmentación. Este error como apuntábamos se podría solventar con un diseño más pormenorizado de las pruebas que se iban a realizar y la manera de recolectar los datos.

7. Futuras líneas de trabajo

Debido a la limitación del espacio donde se ha realizado el estudio una línea interesante para trabajar a futuro es incrementar la distancia entre los saltos inalámbricos para ver como afecta no solo el número de saltos si no también la distancia entre ellos.

Además de la distancia, incrementar el número de saltos inalámbricos y crear redes malladas donde los nodos puedan encaminar los paquetes por diferentes caminos.

Otra línea sería, comparar los resultados con otras marcas de routers para ver cuales tienen mejor rendimiento en las mismas condiciones. Además evaluar otros estándares 802.11 (ej. 802.11n, 802.11ac) y ver si los efectos de las distintas topologías de red mantienen.

8. Apéndices

8.1 Ficheros configuración routers

1. Fichero de configuración ***/etc/config/network*** para 1 router en modo infraestructura:

Router 1:

```
config 'switch' 'eth0'
	option 'enable' '1'

config 'switch_vlan' 'eth0_0'
	option 'device' 'eth0'
	option 'vlan' '0'
	option 'ports' '0 1 2 3 5'

config 'switch_vlan' 'eth0_1'
	option 'device' 'eth0'
	option 'vlan' '1'
	option 'ports' '4 5'

config 'interface' 'loopback'
	option 'ifname' 'lo'
	option 'proto' 'static'
	option 'ipaddr' '127.0.0.1'
	option 'netmask' '255.0.0.0'

config 'interface' 'lan'
	option 'proto' 'static'
	option 'ipaddr' '192.168.1.1'
	option 'netmask' '255.255.255.0'
	option 'type' 'bridge'
	option 'ifname' 'eth0.0 wl0'

config 'interface' 'wan'
	option 'ifname' 'eth0.1'
	option 'proto' 'static'
```

2. Fichero de configuración ***/etc/config/wireless*** para 1 router en modo infraestructura:

Router 1:

```
config 'wifi-device' 'wl0'
    option 'type' 'broadcom'
    option 'txpower' '18'
    option 'channel' '11'
    option 'hwmode' '11bg'
    option 'disabled' '0'

config 'wifi-iface'
    option 'encryption' 'none'
    option 'device' 'wl0'
    option 'ssid' 'TEST1'
    option 'mode' 'ap'
```

3. Fichero de configuración ***/etc/config/network*** para **2 routers** en modo ad hoc:

Router 1:

```
config 'switch' 'eth0'
    option 'enable' '1'

config 'switch_vlan' 'eth0_0'
    option 'device' 'eth0'
    option 'vlan' '0'
    option 'ports' '0 1 2 3 5'

config 'switch_vlan' 'eth0_1'
    option 'device' 'eth0'
    option 'vlan' '1'
    option 'ports' '4 5'

config 'interface' 'loopback'
    option 'ifname' 'lo'
    option 'proto' 'static'
    option 'ipaddr' '127.0.0.1'
    option 'netmask' '255.0.0.0'

config 'interface' 'lan'
    option 'proto' 'static'
    option 'ipaddr' '192.168.1.1'
    option 'netmask' '255.255.255.0'
    option 'ifname' 'eth0.0'

config 'interface' 'wan'
```

```
        option 'ifname' 'eth0.1'
        option 'proto' 'static'

config 'interface' 'wifinet'
        option 'proto' 'static'
        option 'ifname' 'wl0'
        option 'ipaddr' '192.168.2.1'
        option 'netmask' '255.255.255.0'

config 'route'
        option 'interface' 'wifinet'
        option 'target' '192.168.0.0'
        option 'netmask' '255.255.0.0'
        option 'gateway' '192.168.2.2'
```

Router 2:

```
config 'switch' 'eth0'
        option 'enable' '1'

config 'switch_vlan' 'eth0_0'
        option 'device' 'eth0'
        option 'vlan' '0'
        option 'ports' '0 1 2 3 5'

config 'switch_vlan' 'eth0_1'
        option 'device' 'eth0'
        option 'vlan' '1'
        option 'ports' '4 5'

config 'interface' 'loopback'
        option 'ifname' 'lo'
        option 'proto' 'static'
        option 'ipaddr' '127.0.0.1'
        option 'netmask' '255.0.0.0'

config 'interface' 'lan'
        option 'ifname' 'eth0.0'
        option 'proto' 'static'
        option 'netmask' '255.255.255.0'
        option 'ipaddr' '192.168.3.1'

config 'interface' 'wan'
        option 'ifname' 'eth0.1'
        option 'proto' 'dhcp'

config 'interface' 'wifinet'
        option 'proto' 'static'
        option 'ifname' 'wl0'
        option 'ipaddr' '192.168.2.2'
```

option 'netmask' '255.255.255.0'

config 'route'
option 'interface' 'wifinet'
option 'target' '192.168.0.0'
option 'netmask' '255.255.0.0'
option 'gateway' '192.168.2.1'

4. Fichero de configuración ***/etc/config/wireless*** para **2 routers** en modo ad hoc:

Router 1:

config 'wifi-device' 'wl0'
option 'type' 'broadcom'
option 'txpower' '18'
option 'channel' '1'
option 'hwmode' '11bg'
option 'disabled' '0'

config 'wifi-iface'
option 'encryption' 'none'
option 'device' 'wl0'
option 'mode' 'adhoc'
option 'network' 'wifinet'
option 'ssid' 'wlanw'

Router 2:

config 'wifi-device' 'wl0'
option 'type' 'broadcom'
option 'channel' '3'
option 'txpower' '18'
option 'hwmode' '11bg'
option 'disabled' '0'

config 'wifi-iface'
option 'encryption' 'none'
option 'device' 'wl0'
option 'mode' 'adhoc'
option 'network' 'wifinet'
option 'ssid' 'wlanw'

5. Fichero de configuración ***/etc/config/network*** para **3 routers** en modo ad hoc:

Router 1:

```
config 'switch' 'eth0'
    option 'enable' '1'

config 'switch_vlan' 'eth0_0'
    option 'device' 'eth0'
    option 'vlan' '0'
    option 'ports' '0 1 2 3 5'

config 'switch_vlan' 'eth0_1'
    option 'device' 'eth0'
    option 'vlan' '1'
    option 'ports' '4 5'

config 'interface' 'loopback'
    option 'ifname' 'lo'
    option 'proto' 'static'
    option 'ipaddr' '127.0.0.1'
    option 'netmask' '255.0.0.0'

config 'interface' 'lan'
    option 'proto' 'static'
    option 'ipaddr' '192.168.1.1'
    option 'netmask' '255.255.255.0'
    option 'ifname' 'eth0.0'

config 'interface' 'wan'
    option 'ifname' 'eth0.1'
    option 'proto' 'static'

config 'interface' 'wifinet'
    option 'proto' 'static'
    option 'ifname' 'wl0'
    option 'ipaddr' '192.168.2.1'
    option 'netmask' '255.255.255.0'

config 'route'
    option 'interface' 'wifinet'
    option 'target' '192.168.0.0'
    option 'netmask' '255.255.0.0'
    option 'gateway' '192.168.2.2'
```

Router 2:

config 'switch' 'eth0'
option 'enable' '1'

config 'switch_vlan' 'eth0_0'
option 'device' 'eth0'
option 'vlan' '0'
option 'ports' '0 1 2 3 5'

config 'switch_vlan' 'eth0_1'
option 'device' 'eth0'
option 'vlan' '1'
option 'ports' '4 5'

config 'interface' 'loopback'
option 'ifname' 'lo'
option 'proto' 'static'
option 'ipaddr' '127.0.0.1'
option 'netmask' '255.0.0.0'

config 'interface' 'lan'
option 'ifname' 'eth0.0'
option 'proto' 'static'
option 'netmask' '255.255.255.0'
option 'ipaddr' '192.168.5.1'

config 'interface' 'wan'
option 'ifname' 'eth0.1'
option 'proto' 'dhcp'

config 'interface' 'wifinet'
option 'proto' 'static'
option 'ipaddr' '192.168.2.2'
option 'netmask' '255.255.255.0'

config 'route'
option 'interface' 'wifinet'
option 'target' '192.168.1.0'
option 'netmask' '255.255.255.0'
option 'gateway' '192.168.2.1'

config 'route'
option 'interface' 'wifinet'
option 'target' '192.168.4.0'
option 'netmask' '255.255.255.0'
option 'gateway' '192.168.2.3'

Router 3:

config switch eth0
option enable 1

config switch_vlan eth0_0
option device "eth0"
option vlan 0
option ports "0 1 2 3 5"

config switch_vlan eth0_1
option device "eth0"
option vlan 1
option ports "4 5"

config interface loopback
option ifname "lo"
option proto static
option ipaddr 127.0.0.1
option netmask 255.0.0.0

config interface lan
option type bridge
option ifname "eth0.0"
option proto static
option ipaddr 192.168.4.1
option netmask 255.255.255.0

config interface wan
option ifname "eth0.1"
option proto dhcp

config 'interface' 'wifinet'
option 'proto' 'static'
option 'ifname' 'wl0'
option 'ipaddr' '192.168.2.3'
option 'netmask' '255.255.255.0'

config 'route'
option 'interface' 'wifinet'
option 'target' '192.168.0.0'
option 'netmask' '255.255.0.0'
option 'gateway' '192.168.2.2'

6. Fichero de configuración ***/etc/config/wireless*** para **3 routers** en modo ad hoc:

Router 1:

```
config 'wifi-device' 'wl0'
	option 'type' 'broadcom'
	option 'txpower' '18'
	option 'channel' '11'
	option 'hwmode' '11bg'
	option 'disabled' '0'

config 'wifi-iface'
	option 'encryption' 'none'
	option 'device' 'wl0'
	option 'mode' 'adhoc'
	option 'network' 'wifinet'
	option 'ssid' 'wlanw'
```

Router 2:

```
config 'wifi-device' 'wl0'
	option 'type' 'broadcom'
	option 'channel' '11'
	option 'txpower' '18'
	option 'hwmode' '11bg'
	option 'disabled' '0'
config 'wifi-iface'
	option 'encryption' 'none'
	option 'device' 'wl0'
	option 'mode' 'adhoc'
	option 'ssid' 'wlanw'
	option 'network' 'wifinet'
```

Router 3:

```
config 'wifi-device' 'wl0'
	option 'type' 'broadcom'
	option 'txpower' '18'
	option 'channel' '11'
	option 'hwmode' '11bg'
	option 'disabled' '0'

config 'wifi-iface'
	option 'encryption' 'none'
	option 'device' 'wl0'
	option 'mode' 'adhoc'
	option 'network' 'wifinet'
	option 'ssid' 'wlanw'
```

8.2 Scripts de automatización

Cambio de parámetros en los routers

Ejecución del script:

Cambiar_param.sh [-t txpower]\[-c channel]\[-h hwmode]

Contenido script:

```
#Cambio de parámetros
#set -x

USUARIO="root"
IP=""
TXPOWER=""
CHANNEL=""
HWMODE=""
INTERFACE="wl0"
WIRELESS=/home/find/Elena/scripts/wireless
WIRELESS_NEW=/home/find/Elena/scripts/wireless_new
ROUTERS=/home/find/Elena/scripts/routers

MOSTRAR_AYUDA(){

        echo "cambiar_param.sh -t [txpower] -c [channel] -h [hwmode]"
        exit 1
}


while getopts ':t:c:h:' args
do
   case $args in
      t) TXPOWER=$OPTARG;;
      c) CHANNEL=$OPTARG;;
      h) HWMODE=$OPTARG;;
      :) echo "La opcion especificada esperaba un argumento"
        MOSTRAR_AYUDA;;
      \?) echo "Opcion desconocida"
        MOSTRAR_AYUDA;;
   esac
done

while read ROUTER; do

        IP=$ROUTER
        touch $WIRELESS
        touch $WIRELESS_NEW

        scp $USUARIO@$IP:/etc/config/wireless $WIRELESS
```

```
        while  read LINEA; do

                MENSAJE=`echo $LINEA | awk '{ print $2 }'`
                OPTION=`echo $LINEA | awk '{ print $1 }'`
                case $MENSAJE in

                        "'txpower'")
                                if [ "x$TXPOWER" != "x" ]
                                then
                                        echo "   option 'txpower' '$TXPOWER' " >>
$WIRELESS_NEW
                                else
                                        echo "   $LINEA" >> $WIRELESS_NEW
                                fi;;
                        "'channel'")
                                if [ "x$CHANNEL" != "x" ]
                then
                        echo "   option 'channel' '$CHANNEL' " >> $WIRELESS_NEW
                else
                        echo "  $LINEA" >> $WIRELESS_NEW
                fi;;
                        "'hwmode'")
                                if [ "x$HWMODE" != "x" ]
                then
                        echo "   option 'hwmode' '$HWMODE' " >> $WIRELESS_NEW
                else
                        echo "  $LINEA" >> $WIRELESS_NEW
                fi;;
                        *)
                                if [ "$OPTION" = "option" ]
                                then
                                        echo "   $LINEA" >> $WIRELESS_NEW
                                else
                                        echo "$LINEA" >> $WIRELESS_NEW
                                fi
                esac
        done < $WIRELESS

        echo "----------------------------"
        echo "ROUTER: $IP"
        cat $WIRELESS_NEW
        echo "----------------------------"

        echo "/etc/init.d/network restart" > tmp
        echo "/etc/init.d/firewall stop" > tmp
        scp $WIRELESS_NEW $USUARIO@$IP:/etc/config/wireless
        ssh $USUARIO@$IP < tmp

        rm $WIRELESS
        rm $WIRELESS_NEW
      done < $ROUTERS
```

Recogida datos latencia

Ejecución del script:

ping_lab.sh IP

Contenido script:

```
#Recogido información ping
#set -x

NUM_PRUEBA=""
FECHA=`date +"%Y%m%d %H:%M:%S"`
INFRAESTRUCTURA="1 router con wifi"
HOME_SCRIPT="/home/find/Elena/scripts"
HOME_SALIDA="/home/find/Elena/pruebas"
SALIDA_TMP="$HOME_SALIDA/salida_ping.tmp"
SALIDA_TMP2="$HOME_SALIDA/salida_ping2.tmp"
SALIDA_ROUTER="$HOME_SALIDA/salida_router.tmp"
IP=$1
SALIDA_PING="$2"
TIME=""
TXPOWER=""
CHANNEL=""
STANDAR=""


OBTENER_DATOS_ROUTER(){
        USER="root"
        ROUTER="192.168.1.1"
        TMP="$HOME_SALIDA/tmp"
        touch $TMP
        touch $SALIDA_ROUTER
        echo "cat /etc/config/wireless" > $TMP
        ssh $USER@$ROUTER < $TMP > "$SALIDA_ROUTER"
        grep "option" $SALIDA_ROUTER > $TMP
        sed "s/'//g" $TMP > $SALIDA_ROUTER
        echo "salida fichero router"
        cat $SALIDA_ROUTER
        while read LINEA; do
                MENSAJE=`echo $LINEA | awk '{ print $2 }'`
                #echo $MENSAJE
                DATO=`echo $LINEA | awk '{ print $3 }'`
                #echo $DATO
                case $MENSAJE in
                        "hwmode") STANDAR=$DATO;;
                        "txpower") TXPOWER=$DATO;;
                        "channel") CHANNEL=$DATO;;
                esac
```

```
        done < $SALIDA_ROUTER
        echo "TXPOWER=$TXPOWER"
        echo "HWMODE=$STANDAR"
        echo "CHANNEL=$CHANNEL"
        rm $TMP
        rm $SALIDA_ROUTER

}

OBTENER_DATOS_PING(){

        sed "s/time=//" $SALIDA_TMP > $SALIDA_TMP2
    while read LINEA; do
                PRIMERO=`echo $LINEA | awk '{ print $1 }'`
                if [ "$PRIMERO" = "64" ]
                then
                        TIME=`echo $LINEA | awk '{ print $7 }'`
                        ESCRIBIR_CSV
                fi
        done < $SALIDA_TMP2
}

ESCRIBIR_CSV(){

#Si el fichero de salida no existe le añadimos la cabecera
        echo "$SALIDA_CSV"

        if [ ! -e $SALIDA_PING ]
        then
                echo "Fecha, Infraestructura, Num Prueba, txpower, channel, estandar,
latencia" > $SALIDA_PING
        fi
        echo "$FECHA, $INFRAESTRUCTURA, $NUM_PRUEBA, $TXPOWER, $CHANNEL,
$STANDAR, $TIME"
        echo "$FECHA, $INFRAESTRUCTURA, $NUM_PRUEBA, $TXPOWER, $CHANNEL,
$STANDAR, $TIME" >> $SALIDA_PING

}

CONTADOR(){
        NUM_PRUEBA=`tail -1 $HOME_SCRIPT/PID_PING`
    NUM_PRUEBA=`expr $NUM_PRUEBA + 1`
    echo $NUM_PRUEBA > $HOME_SCRIPT/PID_PING
    echo $NUM_PRUEBA
}


if [ "x$IP" = "x" ] || [ "x$SALIDA_PING" = "x" ]
then
        echo "Los argumentos estan incompletos"
else
        echo "ping $IP"
```

```
        ping $IP > $SALIDA_TMP
        OBTENER_DATOS_ROUTER
        CONTADOR
        OBTENER_DATOS_PING
fi
```

Recogida datos pruebas TCP y UDP

Ejecución del script:

Iperf_lab.sh -i [interval] -t [time] -l [buffer] -s [salida] (-w [window] || -u) "

Contenido script:

```
#Recogida información iperf server
#set -x

NUM_PRUEBA=""
FECHA=`date +"%Y%m%d %H:%M:%S"`
INFRAESTRUCTURA="2 router con wifi"
TCP_UDP=""
TXPOWER=""
CHANNEL=""
STANDAR=""
BUFFER=""
BANDWIDTH=""
TRANSFER=""
TCP_WIND_SIZE=""
UDP_BUFFER_SIZE=""
JITTER=""
LOST_TOTAL=""
INTERVAL=""
TIME=""
WINDOW=""
SALIDA_CSV=""
HOME_SCRIPT="/home/find/Elena/scripts"
HOME_SALIDA="/home/find/Elena/pruebas"
SALIDA_TEMPORAL="$HOME_SALIDA/salida_udp.tmp"
SALIDA_ROUTER="$HOME_SALIDA/salida_router.tmp"

MOSTRAR_AYUDA(){

        echo " iper_labf.sh -i [interval] -t [time] -l [buffer] -s [salida] (-w [window] || -u ) "
}

FORMAR_CSV(){
```

```
        NUM_PRUEBA=`tail -1 $HOME_SCRIPT/PID`
        NUM_PRUEBA=`expr $NUM_PRUEBA + 1`
        echo $NUM_PRUEBA > $HOME_SCRIPT/PID
        echo $NUM_PRUEBA

#Separamos por UDP o TCP porque el formato de salida del iperf es diferente

        if [ "$TCP_UDP" = "UDP" ]
        then
                while read LINEA; do
                        MENSAJE=`echo $LINEA | awk '{ print $2 }'`
                        case $MENSAJE in
                  "buffer")
                        UDP_BUFFER_SIZE=`echo $LINEA | awk '{ print $4 " " $5 }'`
                        echo "UDP_BUFFER_SIZE $UDP_BUFFER_SIZE";;
                  "3]")
                        MEN=`echo $LINEA | awk '{ print $3 }'`
                        if [ "$MEN" != "local" ]
                        then
                            LINEA2=`echo $LINEA| cut -d'c' -f2-40`
                                        MEN2=`echo $LINEA2 | awk '{ print $2 }'`
                                        if [ "$MEN2" != "datagrams" ]
                                        then
                                TRANSFER=`echo $LINEA2 | awk '{ print $1 " " $2 }'`
                                BANDWIDTH=`echo $LINEA2 | awk '{ print $3 " " $4 }'`
                                                JITTER=`echo $LINEA2 | awk '{ print $5
" " $6 }'`
                                                LOST_TOTAL=`echo $LINEA2 | awk '{
print $7 "" $8 "" $9}'`
                                echo "TRANSFER $TRANSFER"
                                echo "BANDWIDTH $BANDWIDTH"
                                                echo "JITTER $JITTER"
                                                echo "LOST $LOST_TOTAL "
                                                echo "escribir csv"
                                ESCRIBIR_CSV
                                        fi
                        fi;;
                esac
                  done < $SALIDA_TEMPORAL

        fi
        if [ "$TCP_UDP" = "TCP" ]
    then
                  while read LINEA; do
                MENSAJE=`echo $LINEA | awk '{ print $2 }'`
                        case $MENSAJE in
                                "window")
                                        TCP_WIND_SIZE=`echo $LINEA | awk '{ print $4 " " $5
}'`
                        echo "TCP_WIND_SIZE $TCP_WIND_SIZE";;
                                "4]")
                                        MEN=`echo $LINEA | awk '{ print $3 }'`
```

```
                                        if [ "$MEN" != "local" ]
                                        then
                                                LINEA2=`echo $LINEA| cut -d'c' -f2-40`
                                                TRANSFER=`echo $LINEA2 | awk '{ print $1 " "
$2 }'`
                                                BANDWIDTH=`echo $LINEA2 | awk '{ print $3 "
" $4 }'`
                                                echo "TRANSFER $TRANSFER"
                                                echo "BANDWIDTH $BANDWIDTH"
                                                ESCRIBIR_CSV
                                        fi;;
                                esac
                done < $SALIDA_TEMPORAL


        fi

}

OBTENER_DATOS_ROUTER(){
        USER="root"
        ROUTER="192.168.1.1"
        TMP="$HOME_SALIDA/tmp"
        touch $TMP
        touch $SALIDA_ROUTER
        echo "cat /etc/config/wireless" > $TMP
        ssh $USER@$ROUTER < $TMP > "$SALIDA_ROUTER"
        grep "option" $SALIDA_ROUTER > $TMP
        sed "s/'//g" $TMP > $SALIDA_ROUTER
        echo "salida fichero router"
        cat $SALIDA_ROUTER
        while read LINEA; do
                MENSAJE=`echo $LINEA | awk '{ print $2 }'`
                #echo $MENSAJE
                DATO=`echo $LINEA | awk '{ print $3 }'`
                #echo $DATO
                case $MENSAJE in
                        "hwmode") STANDAR=$DATO;;
                        "txpower") TXPOWER=$DATO;;
                        "channel") CHANNEL=$DATO;;
                esac
        done < $SALIDA_ROUTER
        echo "TXPOWER=$TXPOWER"
        echo "HWMODE=$STANDAR"
        echo "CHANNEL=$CHANNEL"
        rm $TMP
        rm $SALIDA_ROUTER

}

ESCRIBIR_CSV(){
```

```
#Si el fichero de salida no existe le añadimos la cabecera
        echo "$SALIDA_CSV"

        if [ ! -e $SALIDA_CSV ]
        then
                echo "Fecha, Infraestructura, Num Prueba, TCP/UDP, txpower, channel,
estándar, buffer, Bandwidth, Transfer, TCP Windows size, UDP buffer size, Jitter, Lost/Total" >
$SALIDA_CSV
        fi
        echo "$FECHA, $INFRAESTRUCTURA, $NUM_PRUEBA, $TCP_UDP, $TXPOWER,
$CHANNEL, $STANDAR, $BUFFER, $BANDWIDTH, $TRANSFER, $TCP_WIND_SIZE,
$UDP_BUFFER_SIZE, $JITTER, $LOST_TOTAL, $INTERVAL, $TIME"
        echo "$FECHA, $INFRAESTRUCTURA, $NUM_PRUEBA, $TCP_UDP, $TXPOWER,
$CHANNEL, $STANDAR, $BUFFER, $BANDWIDTH, $TRANSFER, $TCP_WIND_SIZE,
$UDP_BUFFER_SIZE, $JITTER, $LOST_TOTAL, $INTERVAL, $TIME" >> $SALIDA_CSV

}


while getopts ':i:t:l:s:w:u' args
do
    case $args in
         i) INTERVAL=$OPTARG;;
                t) TIME=$OPTARG;;
                l) BUFFER=$OPTARG;;
                s) SALIDA_CSV=$OPTARG;;
                w) WINDOW=$OPTARG;;
                u) TCP_UDP="UDP";;
                :) echo "La opcion especificada esperaba un argumento"
           MOSTRAR_AYUDA;;
         \?) echo "Opcion desconocida"
           MOSTRAR_AYUDA;;
    esac
done

if [ "x$INTERVAL" = "x" ] || [ "x$TIME" = "x" ] || [ "x$SALIDA_CSV" = "x" ]
then
        echo "Los argumentos estan incompletos"
        MOSTRAR_AYUDA
else
        if [ "$TCP_UDP" = "UDP" ]
        then
                if [ "x$BUFFER" != "x" ]
                then
                        echo "iperf -s -f m -i $INTERVAL -t $TIME -l $BUFFER -u"
                        iperf -s -f m -i $INTERVAL -t $TIME -l $BUFFER -u > $SALIDA_TEMPORAL
                else
                echo "Los argumentos estan incompletos"
                        MOSTRAR_AYUDA
                fi
        else
                TCP_UDP="TCP"
```

```
                echo "iperf -s -f m -i $INTERVAL -t $TIME -w $WINDOW"
         iperf -s -f m -i $INTERVAL -t $TIME -w $WINDOW > $SALIDA_TEMPORAL
    fi

        if [ -r $SALIDA_TEMPORAL ]
        then
                OBTENER_DATOS_ROUTER
                FORMAR_CSV
        else
                echo "Problema al generar el fichero de salida"
        fi


fi
```

8.3. Desglose tareas y presupuesto

A continuación se hace un desglose de las tareas realizadas en el proyecto y se calcula el presupuesto invertido.

8.3.1 Tareas

A continuación se detalla el desglose de las tareas realizadas en el proyecto y su duración en horas.

- Diseño del proyecto: elección de los parámetros, los escenarios y las pruebas. (40h)
- Configuración de los routers en función del escenario. (60h)
- Automatización de los cambios de parámetros. (50h)
- Automatización de la recogida de resultados. (50h)
- Pruebas. (120h)
- Redacción memoria. (130h)

8.3.2 Presupuesto

En la siguiente tabla se muestran los cargos correspondientes al personal informático cualificado para realizar las distintas tareas o actividades. Todos los costes son calculados sin I.V.A.

Tabla 3: Presupuesto Personal

Apellidos y nombre	Categoría	Dedicación (hombres mes)	Costes hombre mes*	Coste (Euro)
Manchón Pérez, Elena	Ingeniero	3,5	2.694,39	9.430,37
Soto Campos, Ignacio	Ingeniero superior	0,5	4289,54	2144,77
			Total	**11.575,14**

*** 1 Hombre mes = 131,25 horas. Máximo anual de dedicación de 12 hombres mes (1575 horas)**

En la siguiente tabla se muestran los equipos informáticos adquiridos con su coste de amortización durante el periodo que dura el proyecto. Todos los costes son calculados sin I.V.A.

Tabla 4: Presupuesto equipos informáticos

Descripción	Coste (Euro)	Unidades	% Uso dedicado al proyecto	Dedicación (meses)	Periodo de depreciación	Coste imputable*
Router Linksys WRT54GL	**60**	**3**	**100**	**12**	**60**	**12,00**
PC Sobremesa	**800**	**1**	**100**	**12**	**60**	**160,00**
Portátil	**1200**	**1**	**100**	**12**	**60**	**240,00**
					Total	**412,00**

*Fórmula de cálculo de la Amortización:

$$\frac{A}{B} \text{xCxD}$$

A = nº de meses desde la fecha de facturación
B = periodo de depreciación (60 meses)
C = coste del equipo
D = % de uso que se dedica al proyecto

En la siguiente tabla se muestra el sumatorio de los totales anteriormente calculados. A la suma de los costes le vamos a añadir un veinte por ciento en concepto de costes indirectos, lo cual equilibrará los riesgos del proyecto y aquellos otros valores que no se han tenido en cuenta al realizar el presupuesto.

Tabla 5: Presupuesto total del proyecto

Presupuesto Costes Totales	Presupuesto Costes Totales
Personal	9.430
Amortización	412
Subcontratación de tareas	0
Costes de funcionamiento	0
Costes Indirectos	1.968
Total	**11.811**

9. Referencias

[1] IEEE 802.11 Wireless Local Area Networks [Consulta 2-07-2015]. Disponible en: *http://www.ieee802.org/11/*
[2] WI-FI Aliance [Consulta 15-05-2015]. Disponible en:*www.wi-fi.org*.
[3] Cooperación en redes vehiculares. Estado de la cuestión y propuesta de mecanismo basado en incentivo. Sánchez, P. P. (2011). Proyecto Fin de Máster , Universidad Complutense de Madrid. Madrid.
[4] Redes de computadoras, 4a Ed. Tanenbaum, A. (2003). Editorial: Pearson, Prentice Hall.
[5] Influencia del tamaño de paquetes sobre la pérdida de paquetes en un enlace UDP/IP/IEEE 802.11a. Nomar Noroño, José Fermín (2012). Télématique: Revista Electrónica de Estudios Telemáticos, Vol. 11, Nº. 1, págs. 16-26.
[6] Evaluación de prestaciones de una red mallada basada en los dispositivos Linksys WRT54GL. Ramos Santos, F. (2009). PFC Universidad Carlos III, Leganés, Madrid
[7] FloorNet: Deployment and Evaluation of aMultihop Wireless 802.11 Testbed. Serrano, P.; Bernardos, C. J.; de la Oliva, A.; Banchs, A.; Soto, I.; y Zink, M. (2010). EURASIP Journal on Wireless Communications and Networking, Article ID 153102.
[8] Estudio de las variables que influyen para alcanzar el máximo throughput en un trayecto de un sistema inalámbrico multi-salto multicanal. Vásquez Hurtado, J. H. (2012). Rev Acta Nova. Vol. 5 Nº. 4.
[9] Tutorial iperf. [Consulta 20-10-2014] Disponible en: *http://openmaniak.com/es/iperf.php*.

10. Bibliografía adicional

- Configuración equipos Lynksys WRT54G [Consulta: 23-11-2014] Disponible en: *http://www.configurarequipos.com/doc387.html*
- Wireless mesh networks: a survey. Akyildiz, I. F.; Wang, X.; Wang, W. (2005). Computer Networks, Vol. 47, Nº. 4, págs. 445–487.
- Como citar bibliografía. [Consulta 22-07-2015] Disponible en: *http://portal.uc3m.es/portal/page/portal/biblioteca/aprende_usar/como_citar_bibliografia#sitios*